Implementing ADDED ADVANCED ENCRYPTION STANDARD (A-AES) to Secure Data on the Cloud

Mr. Mahendra Kumar Shrivas
Head Of Department, IT
Sikkim Manipal University, Kumasi, Ghana
mahendra@smughana.com

Mr. Satya Vir Singh
Dean – Academics
Sikkim Manipal University, Accra, Ghana
satya@smughana.com

ABSTRACT: ***Cloud Computing is today's and future computing platform. Cloud providers and other third-party brokers are offering cloud solutions to end-users and developers through online marketplace environments [13]. SME's and Large Enterprises are having lots of cloud based services and solutions which can best fit to their business requirement [11]. Enterprises are now migrating to cloud platform [10]. Migration to cloud platform is now part of their strategic and marketing plans. Most of the applications whether it is mobile app, Web App, Embedded App or Office applications are now connected to cloud platform. Cloud based service offering are increasing day by day thus security threats are also increasing. As per Cloud Security Alliance Data Breaches are 1st top most cloud security risk[4].Although data is stored in data center in encrypted form then how hackers manage to decrypt data? In most cases security keys are stored and managed by Cloud Service provider which invites another security risk Insider Attack which is 6th top most cloud security risk [5]. Most of the providers are using 128 & 256 bit long security key which is not strong and can be broken with various techniques [12].***

In this research paper we are implementing ADDED ADVANCED ENCRYPTION STANDARD (A-AES) [12] algorithms to secure data on cloud platform which uses relatively much stronger keys and suggesting let cloud end user manage the security key to restore trust over profit.

KEYWORDS: Cloud Computing, Cloud Security, A-AES, AES, Encryption, Decryption, Data Security

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models [15].

Five Essential Characteristics:-

1. On-demand self-service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured service

Three Service Models:-

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

Four Deployment Models:-

1. Private cloud
2. Community cloud
3. Public cloud
4. Hybrid cloud

Now Cloud Computing has become a scalable services consumption and delivery platform in the field of Services Computing. The technical foundations of Cloud Computing include Service-Oriented Architecture (SOA) and Virtualizations of hardware and software. The goal of Cloud Computing is to share resources among the cloud service consumers, cloud partners, and cloud vendors in the cloud value chain. The resource sharing at various levels results in various cloud offerings such as infrastructure cloud (e.g. hardware, IT infrastructure management), software cloud (e.g. SaaS focusing on middleware as a service, or traditional CRM as a service), application cloud (e.g. Application as a Service, UML modeling tools as a service, social network as a service), and business cloud (e.g. business process as a service) [8].

Cloud based service offering are increasing day by day. Many studies indicate that more than 50 percent of all information technology will be in

the cloud within five to 10 years. While it's important everywhere, it's even more important for emerging markets [7]. The IEEE wants the cloud to grow like the Internet. Twenty-one global companies and research institutions have joined the IEEE Intercloud Testbed and launched work to create a diverse, interoperable, and federated cloud. Results from the project will also assist in the development of the forthcoming IEEE P2302™ Standard for Intercloud Interoperability and Federation, which is developing standard methodologies for cloud-to-cloud interworking [9]

II. CLOUD COMPUTING THREATS AND VULNERABILITIES

As Cloud Computing related technologies are evolving and growing in different verticals security threads and vulnerabilities are also increasing accordingly. Over the years the number of cloud vulnerability incidents has risen as shown in figure 1[16]. In fact from 2009 to 2011 the number of cloud vulnerability incidents more than doubled - from 33 to 72, most likely due to the phenomenal growth in cloud services [4].

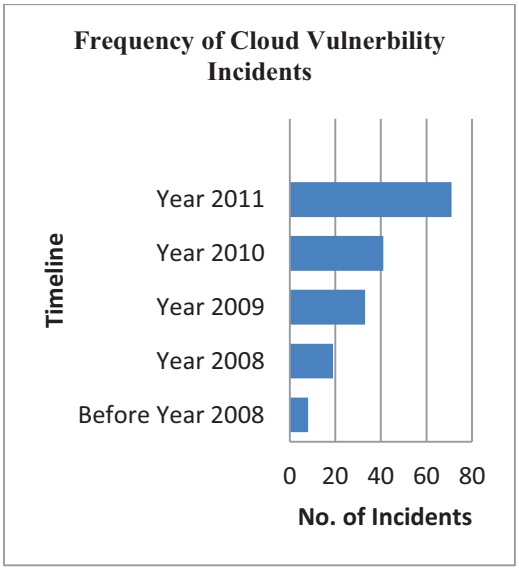

Figure 1: Frequency of Cloud Vulnerability Incidents

The investigation revealed that the top three threat were "Insecure Interfaces & API" (51 incidents; 29% of all threats), "Data Loss & Leakage" (43 incidents; 25%), and "Hardware Failure" (18 incidents; 10%). These three threats accounted for 64% of all cloud outage incidents.[12]. After a thorough review of reported incidents, 128 incidents were grouped into the 8 threats contained in the Top Threats Report while 44 incidents were unable to be categorized.

As such, the authors propose five new categories to accommodate the remaining 44 incidents: Hardware Failure, Natural Disasters, Closer of Cloud Service, Cloud-related Malware and Inadequate Infrastructure Design and Planning [16]. As per The Cloud Security Alliance Top Threats Working Group following are the top identified critical threats to cloud security [5]:-

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issues

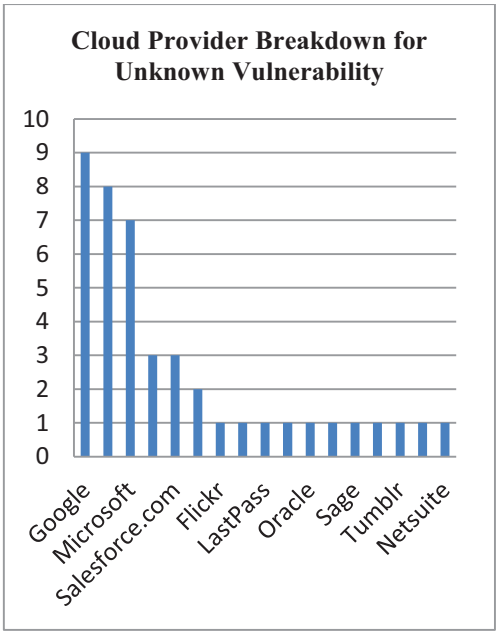

Figure 2: Cloud Provider Breakdown for Unknown Vulnerability

III. PROBLEM SPECIFICATION

Some of The Cloud Threats are still unknown which can be more harmful. As mentioned in figure 2[10] all major cloud service providers reported vulnerabilities which is still unknown. It can be more dangerous as vulnerabilities are unknown one cannot plan to avoid or stop these threats and the whole cloud infrastructure left in high risk. One successful attack can lead to big Data Breaches. What makes it more worse? Most of the cloud venders store security key in their server along with encrypted data. A malicious insider, such as a system administrator, in an improperly designed cloud scenario can have access to potentially sensitive information.

From IaaS to PaaS and SaaS, the malicious insider has increasing levels of access to more critical systems, and eventually to data. Systems that depend solely on the Cloud Service Provider(CSP) for security are at great here. Even if encryption is implemented and are only available at data usage time, the system is still vulnerable to malicious insider attack.[4] Most of the providers are using 128 & 256 bit long security key [14] which is not strong and can be broken with various technique [12]. Cloud service providers deliver their services in as scalable way by sharing infrastructure, platforms and applications. Whether it's the underlying components that make up this infrastructure(e.g. CPU caches, GPU, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture(IaaS), re-deployable platforms (PaaS), or multi-customer application (SaaS), the threat of shared vulnerabilities exists in all delivery model. Cloud based Virtual Machine could be used to extract private cryptographic keys being used in other virtual machines on the same physical server. If a multitenant cloud service database is not properly designed, a flaw in one client's application could allow an attacker access not only to that client's data, but every other client's data as well [5]. As part of disaster management strategy cloud provides keep backup of clients data and security key in multiple locations which leads to more security threats.

IV. PROPOSED SOLUTION

What is the primary motivation behind top most threats like Data Breaches, Account Hijacking, and Malicious Insiders?

To gain access of data of target victims for competitive business advantage or make lots of money after selling those hacked information to target's business rivals. Lots of the attacks are motivated and funded by various governments, organized cyber criminals and security firms.

Most of the identified and unknown security threats and vulnerabilities can be solved using following two simple strategy **:-**

1.Uses of complex and strong encryption algorithm

2. By storing security key in the Client side
(In the system which is not connected to the Internet)

As explain in figure-3, In case of data breaches and malicious insider attack without security key encrypted data cannot be decrypted. Due to complex and strong encryption algorithm it is almost impossible to decrypt the encrypted data. If Cloud Account is hijacked then also hacker can't decrypt data on cloud as it is encrypted before uploading it to cloud and key is not stored on the cloud.

As part of solution we are implementing ADDED ADVANCED ENCRYPTION STANDARD (A-AES) [4] algorithm which is strong enough to secure data on the cloud.

V. SYSTEM DESIGN

Proposed system is designed to use ADDED ADVANCED ENCRYPTION STANDARD (A-AES) algorithm. In A-AES algorithm, the length of the input block, the output block and the State is 512 bits. This is represented by *Nb* = 8, which reflects the number of 64-bit words (number of columns) in the State.

For the A-AES algorithm, the length of the Cipher Key,

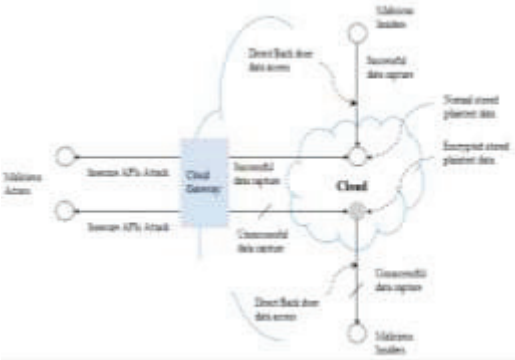

Figure 3: Different between unencrypted and encrypted cloud store

K, is 512, 768, or 1024 bits. The key length is represented by ***Nk*** = 8, 12, or 16, which reflects the number of 64-bit words (number of columns) in the Cipher Key.

For the A-AES algorithm, the number of rounds to be performed during the execution of the algorithm is dependent on the key size. The number of rounds is represented by ***Nr***, where ***Nr*** = 18 when ***Nk*** = 8, ***Nr*** = 22 when ***Nk*** = 12, and ***Nr*** = 26 when ***Nk*** = 16. [4]

The only Key-Block-Round combinations that conform to this standard are given below [4] :-

	Key Length (Nk words)	**Block Size (Nb words)**	**Number of Rounds (Nr)**
A-AES-512	8	8	18
A-AES-768	12	8	22
A-AES-1024	16	8	26

Figure 4: Relation between key length, block size and number of rounds

Proposed System has following two major process :-

1. A-AES Encryption and Uploading Process
2. Downloading and A-AES Decryption Process

Both processes are depicted in Fig5 and Fig6. As mentioned in Fig5 and Fig6 End User have to enter security key manually at the time of A-AES encryption and decryption. In the proposed system there isn't any option to store security key. End User have to maintain a list of file name and security key being used in the process separately.
We are recommending to use different systems to store the list and do not connect the system to the Internet for the security of the key.

VI. IMPLEMENTATION

The whole system is implemented keeping re-usability in mind. We have used Amazon S3 cloud store service and using Amazon S3 based API for Java development. We have developed Application Programming Interface (API) for A-AES algorithms and for Amazon S3 interaction. Graphical Interface is implanted using Java Swing and visual validation technique is used to depict system errors and exceptions. We are using new file extension **.maha** to store intermediate cipher text.

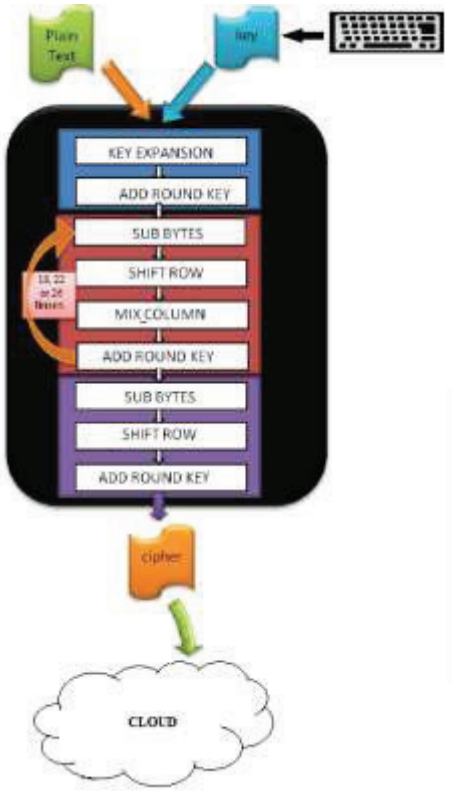

Figure 5: A-AES Encryption and Uploading Process

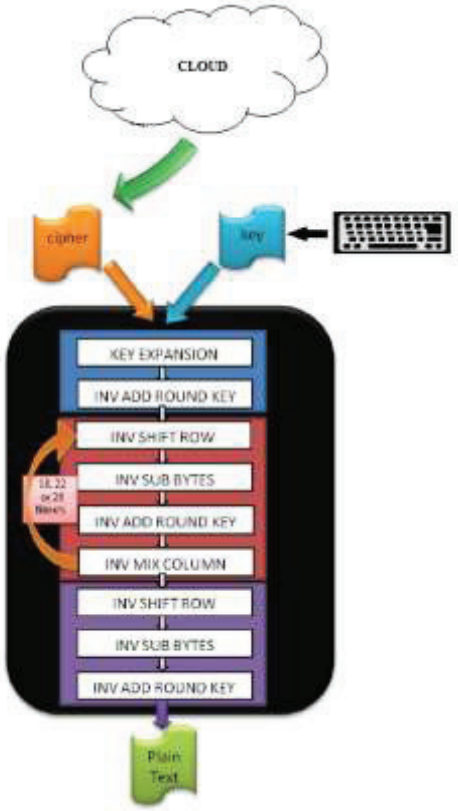

Figure 6: Downloading and A-AES Decryption Process

System is designed to work with any size of plain text files. End user is allowed to choose any plain text file from their computer system. As per as A-AES security key is concern it must

be 64(512 bit), 96(768 bit) or 128(1024 bit) characters long.

After reading 512 bits of data block at a time A-AES encryption is applied and stored in an intermediate file with **.maha** file extension. Original file name is maintained with extension for end user flexibility. Naming of intermediate file is mentioned below :-

- **Original File Name With Extension + .maha**

At the end if data block is less than 512 bits it is written as it is in the intermediate file as current implementation strictly work with 512 bit data block with no padding.

Then after user's Amazon Web Services (AWS) S3[3] credential is validated from credential file which is stored in users home directory[2]. After successful authentication intermediate encrypted file is uploaded into specified cloud store of S3 if specified store is already available for specified user or else it will create new store with the name if name does not exist and is valid as per Amazon S3 naming rules[1].
User is notified once uploading process is completed or error message is generated with reason of error as shown in Fig7.

Intermediate encrypted file is available in client machine as a backup do avoid any data lost threat [4] which may occur at cloud service provider end.

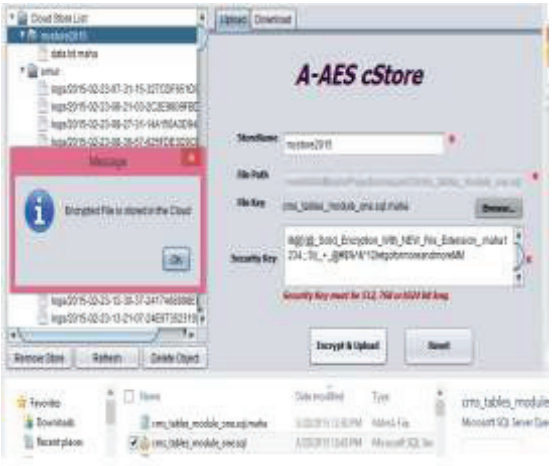

Figure 7: Screenshot of A-AES Encryption and Uploading Process

As file is stored in the cloud in encrypted form and key is not stored in the cloud insider attacker and hacker may download encrypted data after successful attack from the cloud but without key it is impossible to break the encryption unless they invest lots of money, electricity and many years.

Encrypted data can be download by specifying the store name, file to be downloaded and target file name and location as depicted in Fig8

If security key is not correct then also system will allow to download the file from the cloud but it will add one more layer of encryption into it instead of decryption.
In case of security key is correct system downloads 512 bits of data block from the cloud and after encryption it writes back the data into target file.

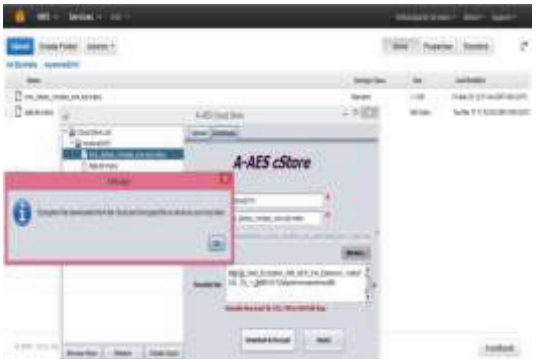

Figure 8: Screenshot of Downloading and A-AES Decryption Process

At the end if data block is less than 512 bits it is written directly to the target file without encryption. Plain text, cipher text and decipher text can be seen in Fig.9.

Figure 9: Plain Text, A-AES Cipher Text, Decipher Text

In Fig. 10 Input Text, A-AES Key, A-AES Cipher Text and Decipher Test is given for 512bit, 768 bit and 1024 bit A-AES Key.

Plain Text
000102030405060708090A0B0C0D0 E0F11121314151617180A1A2A3A4A 5A6A7A0B1B2B3B4B5B5B7B0C1C2C 3C4C5C6C7C0D1D2D3D4D5D6D7D0E 1E2E3E4E5E6E7E
A-AES 512 bit Key

000102030405060708090A0B0C0D0E0F10111213141516170B1B2B3B4B5B5B7B22232425262728291 11B2B3B4B5B5B7B323334354E5E6E7E221B2B3B4B5B5B7B
Cipher Text
CB2C244437C9D1A66C98FD9F7AE9874B89BD71352D76B961B58A3BE5EE85F5026918377040757 2B7F14D3B7221C7161B503C7B5FB46685A8CAA632D2D5C37E38
Decipher Text
000102030405060708090A0B0C0D0E0F11121314151617180A1A2A3A4A5A6A7A0B1B2B3B4B5B5B7B0C1C2C3C4C5C6C7C0D1D2D3D4D5D6D7D0E1E2E3E4E5E6E7E
Plain Text
000102030405060708090A0B0C0D0E0F11121314151617180A1A2A3A4A5A6A7A0B1B2B3B4B5B5B7B0C1C2C3C4C5C6C7C0D1D2D3D4D5D6D7D0E1E2E3E4E5E6E7E
A-AES 768 bit Key
000102030405060708090A0B0C0D0E0F10111213141516170B1B2B3B4B5B5B7B22232425262728291 11B2B3B4B5B5B7B323334354E5E6E7E221B2B3B4B5B5B7B424344454E5E6E7E331B2B3B4B5B5B7B525354554E5E6E7E441B2B3B4B5B5B7B
Cipher Text
E6B5FAEFE69CAA232218613810995 9A1C28711538916F29E46F0974AE321ACE924F3B564C103A115329ABE6480B34E8237A80970083CD7CDDCBCF133A5D11617
Decipher Text
000102030405060708090A0B0C0D0E0F11121314151617180A1A2A3A4A5A6A7A0B1B2B3B4B5B5B7B0C1C2C3C4C5C6C7C0D1D2D3D4D5D6D7D0E1E2E3E4E5E6E7E
Plain Text
000102030405060708090A0B0C0D0E0F11121314151617180A1A2A3A4A5A6A7A0B1B2B3B4B5B5B7B0C1C2C3C4C5C6C7C0D1D2D3D4D5D6D7D0E1E2E3E4E5E6E7E
A-AES 1024 bit Key
000102030405060708090A0B0C0D0E0F10111213141516170B1B2B3B4B5B5B7B22232425262728291 11B2B3B4B5B5B7B323334354E5E6E7E221B2B3B4B5B5B7B424344454E5E6E7E331B2B3B4B5B5B7B525354554E5E6E7E441B2B3B4B5B5B7B626364654E5E6E7E551B2B3B4B5B5B7B727374754E5E6E7E661B2B3B4B5B5B7B
Cipher Text
84431C5A9DB472AEB97483E4BA9BC23FF015C1FC2153BD1983A65176BEF3377FCCA71D0C97806B6F0BBC3314B7A49F16E1EFC048CB633EA4C9D0E1C537B60BD1
Decipher Text
000102030405060708090A0B0C0D0E0F11121314151617180A1A2A3A4A5A6A7A0B1B2B3B4B5B5B7B0C1C2C3C4C5C6C7C0D1D2D3D4D5D6D7D0E1E2E3E4E5E6E7E

Figure 10: Plain Text, A-AES Keys, A-AES Cipher Text, Decipher Text

VII. CONCLUSION AND FUTURE WORK

Cloud Computing is emerging technology. No doubt it has lots of services to offer and more cloud related services are about to come. Security in the Cloud is the biggest issue. However as per experts more than 50% IT infrastructure will be in the Cloud in next five years. Threats and Vulnerabilities in the Cloud is the biggest hurdle in the adoption of the Cloud regardless of IT investment and operation cost benefits. Adoption of cloud is directly linked with the question "Do we want to compromise our data over profit?".
Uses of strong encryption algorithms like A-AES and offline storage of security key can save end users of the Cloud from the threats like Data Breaches, Data and Traffic Hijacking and Malicious Insiders which are biggest user concerns also.

Although the current system is experimental which is designed to encrypt and decrypt plain text only. In the real working system it can be extended to encrypt and decrypt all files and media formats. It can be implemented in all java supported devices.

VIII. REFERENCES

[1] Amazon Simple Storage Service Developer Guide (API Version 2006-03-01) Retrieved., 20th March 2015, from http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html

[2] Amazon Simple Storage Service Developer Guide (API Version 2006-03-01) Retrieved., 20th March 2015, from http://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html

[3] Amazon Simple Storage Service (2015) Retrieved., 20th March 2015, from http://aws.amazon.com/s3/

[4] Babcock, C. (2009) Cloud Implementation To Double By 2012. Retrieved, 8th March 2015, from http://www.informationweek.com/news/services/saas/214502033?queryText=cloud

[5] Cloud Security Alliance (2010) Top Threats to Cloud Computing (V1.0), Retrieved., 9th March 2015, from https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[6] Cloud Security Alliance Top Thread to Cloud Computing (November 2013) Retrieved 4 March 2015, from https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

[7] Gopal Pingali, IEEE International Conference on Cloud Computing for Emerging Markets (CCEM)'s conference chair (October 2013) Retrieved 7th March 2015, from http://theinstitute.ieee.org/benefits/conferences/for-emerging-markets-a-focus-on-the-cloud

[8] IEEE 6th International Conference on Cloud Computing (July 2013) Retrieved 6 March 2015, from http://www.thecloudcomputing.org/2013/history.html

[9] IEEE INTERCLOUD TESTBED PROJECT ANNOUNCES FOUNDING MEMBERS (October, 2013) Retrieved, 7th March 2015, from http://cloudcomputing.ieee.org/intercloud/press-release

[10] Khajeh-Hosseini, Greenwood, Sommerville, (2010) Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on DOI: 10.1109/CLOUD.2010.37

[11] Kloch, C., Petersen, E. B and Madsen O. B. (2011) "Cloud Based Infrastructure, the New Business Possibilities and Barriers," Wirel. Pers. Commun., vol. 58, pp. 17-30

[12] Mahendra Kumar Shrivas, Satya Vir Singh (April , 2014) ADDED ADVANCED ENCRYPTION STANDARD (A-AES): With 512 bits data block and 512, 768 and 1024 bits encryption key International Journal of ICT and Management (IJICTM) ISSN No. 2026-6839

[13] Margaret Rouse (November 2013) Retrieved 4th March 2015 , from http://searchcloudprovider.techtarget.com/definition/cloud-marketplace

[14] Nikos Virvilis, Stelios Dritsas, Dimitris Gritzalis, (2011)Secure Cloud Storage, TrustBus'11 Proceedings of the 8th International Conference on Trust, Privacy and Security in digital business, Springer-Verlag Berlin

[15] Peter Mell, Timothy Grance (September 2011)The National Institute of Standards and Technology(NIST) Definition of Cloud Computing, Special Publication 800-145

[16] Ryan Ko, Stephen S G Lee (August 2012, Revised March 2013) Cloud Computing Vulnerability Incidents: A Statistical Overview, 2013 Could Security Alliance, pp. 6-11

AUTHORS PROFILE

Mahendra Shrivas has over 9 years of experience in IT Education and Industrial ICT curriculum development and Project Trainings along with software product and web component development. He started his career in IT industry with NIIT Limited and worked as a Technical Head and also worked as a Software Engineer in one of the leading Software firm of Central India. During his association with HCL Infosystems he has visited various top ranking Universities and Engineering Colleges and conducted ICT and Project Trainings in various technologies. Prior to his current assignment he worked as Sr. Subject Matter Expert with GGITM (Gyan Ganga Institute of Technology and Management) and had mentored various academic research projects sponsored by Microsoft and IBM. Apart from teaching and project mentoring his key strengths include Open Source Innovation and Cyber Security. He is also a Mozilla Rep and represents Ghana for Open Source Learning and Web Literacy.

Satya Vir Singh has over 15 year experience as an accomplished academician with rich experience in IT Training, Designing & Development with Education vertical and fostering tie-ups of Educational institutions. He is highly passionate, result oriented young energetic leader with great respect for people, process and innovation. Prior to his present assignment he was associated with NIIT Ghana, NIIT Ltd - India and B.K Birla Centre for Education – Qatar and Air Force Schools in India. Currently he is working with Academic City College (formerly known as SMU Ghana Learning Centre) Ghana as Dean - Academics.