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 8, August 2017

A Survey on Plausible Approach to Mitigate Security Challenge in Cloud Computing

Ejem Agbaeze, Dr. Nwokorie E.C., Njoku Donatus, Dr. Odii J.N., Nwokoma F.O.

Assistant Lecturer, Department of Computer Science, School of Physical Sciences, Federal University of Technology Owerri, Imo State, Nigeria

Senior Lecturer, Department of Computer Science, School of Physical Sciences Federal University of Technology Owerri, Imo State, Nigeria

Ph.D Student, Department of Computer Science, School of Physical Sciences Federal University of Technology Owerri, Imo State, Nigeria

Senior Lecturer, Department of Computer Science, School of Physical Sciences Federal University of Technology Owerri, Imo State, Nigeria

Assistant Lecturer, Department of Computer Science, School of Physical Sciences Federal University of Technology Owerri, Imo State, Nigeria

ABSTRACT: Cloud Computing is an adaptable, beneficial, tested and demonstrated stage for conveying businesses or end-users Information Technology (IT) administration and management over the Internet. Be that as it may, Cloud Computing usage is rising very quickly and raising various security challenges throughout today's reality. In cloud computing, the security challenges inherent incorporates security and secrecy of end-user data and also the area where data resides, its movement, its accessibility and so on. There are different perspective and feelings on the security of data in the cloud. Hence, this paper presents plausible approaches in cloud computing to mitigate these security challenges, utilizing a broad research methodology. Data was gathered and broken down from recognized writings, standard records, industry periodicals, white papers and experts' report. The approaches tackle the problem of protecting data-in movement, in procedure, and at time-out. It as well deal with securing platform that extents trust across federated clouds, selecting the best service provider, etc. It was also found that using these approaches counter-measure the security challenges in cloud computing to a great extent.

KEYWORDS: Cloud Computing, Security Challenges, Internet, encryption, Data protection

I. Introduction

The significance of Cloud Computing is expanding and it is getting a developing consideration and implementation across the computing world. Cloud Computing allows pervasive, helpful, immediate-response system access to a common pool of computing resources (e.g., systems on network, servers, applications, and administration etc.) that can be provisioned and discharged with insignificant control from the administrators. Figure 1 is the diagrammatic delineation of Cloud Computing.

As indicated by Rosado, et al [1] and Zhao, et al [2], Cloud Computing shows up as a computational worldview including the conveyance design and its principal target is to give secure, fast, advantageous information stockpiling and net registering administration, with all processing assets pictured as service and conveyed over the internet. The cloud improves cooperation, spryness, versatility, accessibility, capacity to adjust to variances as per interest, quicken advancement work, and gives potential to cost lessening through enhanced and productive computing. In spite of the fact there are numerous advantages to receiving cloud computing, there are additionally some huge hindrances to its reception. It has standout amongst the most critical obstructions to its reception is security, trailed by issues with

DOI: 10.15680/IJIRCCE.2017. 0508020

respect to consistence, protection and legitimate matters. The way that cloud computing speaks to a generally new processing model, there is a lot of instability about how security at all levels (e.g., network systems, host, application, and information levels) can be accomplished and how applications security is moved to cloud computing [1]. That vulnerability reliably driven data administrator to express that security is there number one worry with cloud computing [3].

II. RELATED WORK

A. Cloud Computing.

Cloud computing has been the most recent expansion of a development in distributed computing that exploits the propels of technological innovation. The cloud's roots emanated from mainframe computational processing, which was use as servers to manage and control the activities of other computers or terminal connected to it as defined by the operating system. The coming of speedier and less expensive chips, Random Access Memory, storage devices took computing to a new paradigm shift of client –server model that uses a server to share all the resources within the network. These network systems interconnected to form the internet as transfer speed turned to be omnipresent, speedier, and less immoderate. IT divisions normally procure their datacenters in house, and henceforth are secured inside a firewall. In the long run, ventures exploited higher throughput to rethink the requirements for solid on location datacenters. Getting to servers for all intents and purposes through a program window present generous favourable circumstances in software and hardware upkeep. Software merchants started gaining the idea that scaled datacenter could likewise convey remote substance to clients very quickly at a diminished cost, leading to immediate-response Software-as-as-Service. Today's experienced virtualization infrastructures allow modern cloud computing: another model for fast, immediate-response, minimal effort, distributed computing. Like its forerunners, present-day cloud computing includes a large number of client associated with remote assets over the Internet. Cloud computing conveys software and administrations or services over systems on network , depending on a relentless stream of throughput to and from the virtualized datacenter keeping in mind the end goal to keep up high administration or service levels. Kresimir and Zeljko [4] talked about abnormal state of security in the cloud computing model, for example, data trustworthiness, installment and protection of delicate data. Subashini and Kavitha [5] examine the security difficulties of the cloud administration or service conveyance model, concentrating on the SaaS model. A present overview by Cloud Security Alliance (CSA) [6] & Institute of Electrical and Electronic Engineers (IEEE) shows that ventures crosswise over segments of global computing are anxious to embrace cloud computing yet that security are required both to quicken cloud appropriation on a wide scale and to react to administrative drivers. It also worth noting that cloud computing is molding the fate of IT yet the nonattendance of a consistence situation is having emotional effect on cloud computing development. According to Kevin et al [7], there are various security issues for cloud computing as it envelops numerous technological advancements including network system, databases, virtualization, load balancing, etc. accordingly, security issues for many of these frameworks and innovations are relevant to cloud computing. The primary issues they considered incorporates storage security, middleware security, data security, network security and application security. The fundamental objective is to safely store and oversee data that is not controlled by the proprietor. Studies have been done to identifying with the security issues in cloud computing but this work presents a detailed survey of the plausible approaches to countermeasure cloud computing security issues and challenges.

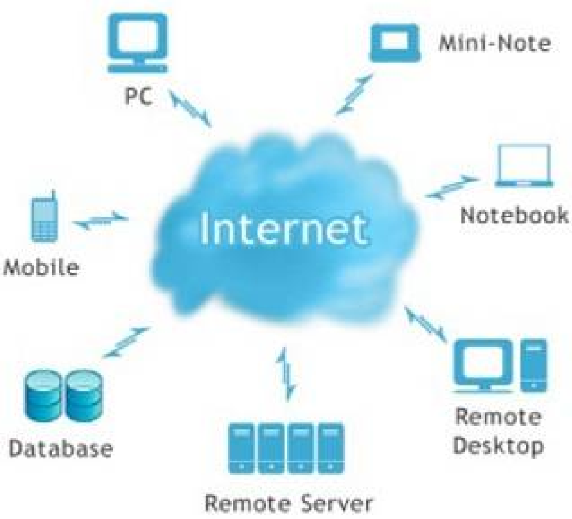

Figure 1: Cloud Computing [8]

B. **Types of Cloud Computing**

Private Cloud

Private cloud is another term that a few merchants have presently used to depict offerings that imitate cloud computing on private network systems. It is implemented inside an associations' inward endeavour datacenter. In private cloud, adaptable assets and virtual applications gave the cloud seller are pooled together and accessible for cloud clients share and utilize. It differs from public cloud in that all the cloud resources and applications are overseen by the association, like Intranet usefulness. Usage on private cloud can be of a great deal and more secure than that of public cloud in view of its predetermined inner presentation. The association that assigned partners might have admittance to work on particular private cloud [9].

Public Cloud

A public cloud is implemented over the Internet, which can begotten by any client who has paid for the service provider [10]. Public clouds are owned by internet service providers. They are made use of by membership or subscription. Numerous organization have fabricated public cloud, to be specific Google App Engine, Amazon AWS, Microsoft Azure, IBM Blue Cloud, and Sales force Force.com. It is normally in view of a pay-per-use model, like a prepaid power metering framework which is sufficiently adaptable to take care of spikes popular for cloud enhancement. Public clouds are less secure than the other cloud models since it puts an extra weight of guaranteeing all applications and data accessed on public cloud are not subjected to malevolent assaults.

Hybrid Cloud

Hybrid cloud is a private cloud connected to more than one outside cloud platforms, centrally controlled, provisioned as a solitary unit, and encircled by a safe network. It gives virtual IT arrangement through a blend of both public and private clouds. Hybrid Cloud provides more secure control of data and applications and permits different groups to get to data over the Internet. In additionally it has an open architecture that permits interfaces with other administration frameworks.

Hybrid cloud can describe configuration joining a local device, for example, a Plug computer with cloud services. It can likewise depict designs joining virtual and physical, assembled resources -for instance, a mostly virtualized environment that requires physical servers, routers, or other hardware network appliance that acts as a firewall or spam filter [9]. Figure 2 illustrates types of cloud computing.

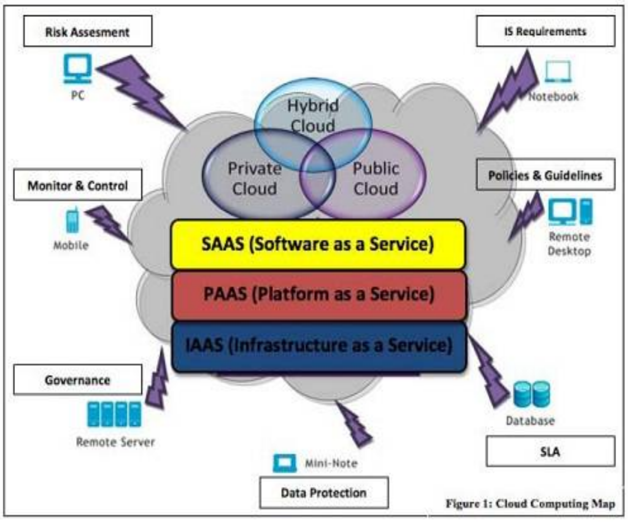

Figure 2: Cloud Deployment Model [11]

C. Services of Cloud Computing

There are three administrations or service models for cloud computing [12] as appeared in figure 2 which outlines how computing assets or power are being procure and devoured as a utility taken account of the prior layout attributes. The service models are:

*Software as a Service (SaaS)***:** This gave the end user access to use the internet service provider's applications running on a cloud infrastructure. The applications are open from different customer gadgets through a meager client interface, for example, web browser (e.g., Web-based email). The customer does not oversee or control the hidden cloud infrastructure including network, servers, operating systems, storage, or even individual application abilities, with the conceivable exemption of constrained client particular application setup settings. Illustrations of SaaS are: CRM, HR or Accounting application.

Platform as a Service (PaaS): This capacity gave the customer to send to the cloud infrastructure customer-created or -procured applications created using programming languages and tools supported by the service provider. The consumer does not oversee or control the hidden cloud infrastructure including network, servers, operating systems, or storage, but has control over sent applications and possibly application hosting environment configurations, e.g. Microsoft Azure, SalesForce or Amazon web service and host of others.

Infrastructure as a Service (IaaS): This gave the customer provisional processing, storage, networks, and other fundamental computing resources where customers are able to send and run arbitrary software, which can incorporate operating systems and applications. The consumer does not oversee or control the hidden cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host, firewalls). Illustration of IaaS provider are Rackspace Hosting, Network Solution, Go-daddy Hosting

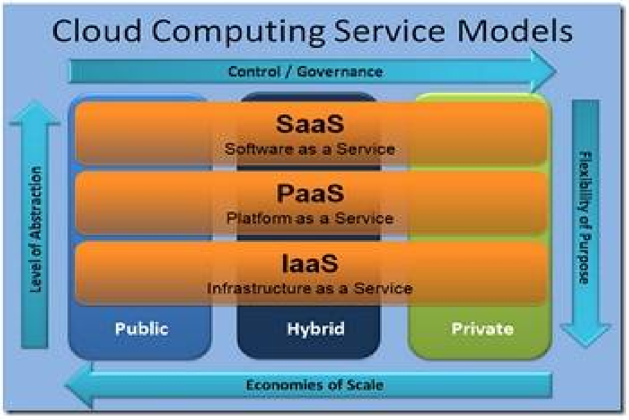

Figure 3: Cloud Computing Service model [12]

III. SECURITY CHALLENGES IN CLOUD COMPUTING

In customary server farms, IT directors put techniques and controls set up to assemble a solidified border around the framework and information they need to secure. This design is moderately simple to oversee, since associations have control of their servers' area and use the physical equipment totally for themselves. In the private and public cloud, be that as it may, border limits obscure and control over security reduces as applications move progressively and associations have the same remotely found physical equipment with outsiders [13].

Multi-Tenancy

Cloud computing clients offer physical assets with others through regular programming or software virtualization layers. These common infrastructure bring one of a kind dangers into an end-user's asset stack. For instance, the cloud end-user is totally ignorant of a neighbour's character, security profile or expectations. The virtual machine running besides the end-user surroundings could be vindictive, hoping to assault alternate hypervisor tenants or sniff correspondences moving all through the framework. Since the cloud customer's information sits on regular storage or stockpiling equipment, it could get to be traded off through careless access administration or malevolent assault.

Multi-location of the private data

It is somewhat unsafe, if the business stores its private information in the outsider's gadget. In this sense, the organizations' private information are sitting in another person's PC, and in another person's office. At that point, numerous things can turn out badly. Firstly, the cloud administration supplier might leave business. Also, the cloud administration supplier might choose to hold the information as prisoner if there is a misunderstanding. Thirdly, it is somewhat vital for an organization to comprehend in which nation its information will be stationed [14].

Cookie Poisoning

It includes changing or adjusting the substance of cookies to have an unapproved access to an application or to a webpage. Cookies fundamentally contain the clients personality related certifications and once these cookies are open, the substance of these cookies can be fashioned to mimic the approved clients Figure 4 delineates this sort of assault

Data Privacy

The general population nature of cloud computing has a huge ramifications on information protection and secrecy. Cloud data is frequently put away in plain content, and few organizations have a flat out comprehension of the affectability levels their information stores hold. Information ruptures are humiliating and unreasonable. Truth be told, a present report by the Cloud Security Alliance records information misfortune and spillage as one of top security worries in the cloud.

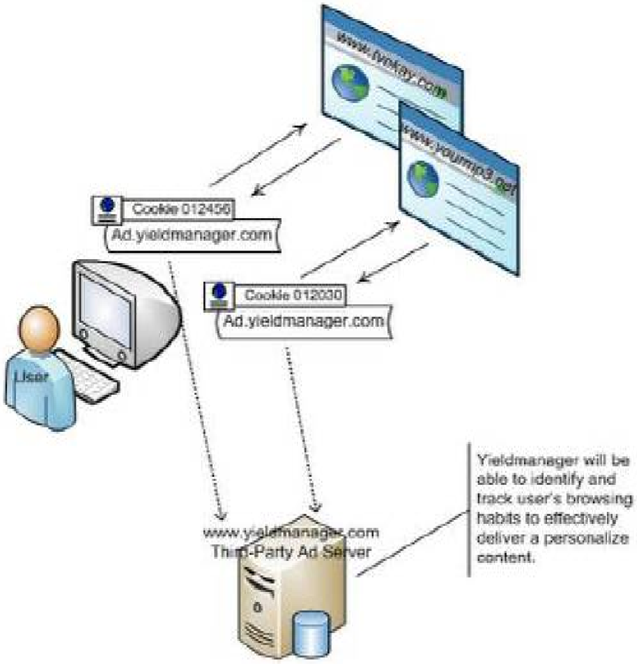

Figure 4: Cookie Poisoning [15]

Present laws, regulations and compliance systems exacerbate the dangers; erring organizations will be made to take charge of the loss of touchy or sensitive information or data and might be confronted with substantial fines over data or information ruptures. Apart from the dent loss of data placed on businesses, it also has negative effects on an individual level. Stolen medical records or history, ATM card numbers or bank data might bring about enthusiastic and monetary ruin, the repercussions of which could take years to repair. Touchy data put away inside of cloud platforms must be shielded to secure its proprietors and subjects alike.

IV. APPROACHES TO SECURITY CHALLENGES IN THE CLOUD

A Protect Data- In Movement, In Procedure, and time-out

Encryption is a viable, entrenched approach to ensure the safety of touchy information. It is generally viewed as a best practice to utilize encryption on any touchy data that may be at danger of loss of physical control-for instance, numerous organizations have strategies that information on portal PCs must be encoded. It is fundamentally critical in cloud platforms— particularly in hybrid or public cloud service models, where information might move outside the conventional IT environment, additionally in inward private clouds, where data can be uncovered on shared process assets.

Certain commercial ventures, for example, social insurance and money related administrations, oblige organizations to meet certain regulations and standards for the way they secure data. Progressively, these and different regulations are empowering—and indicating—encryption in certain utilization situations, including cloud computing. The punishments for rebelliousness are stiffer than at any other time. Moreover, information encryption is frequently not utilized extensively because of the execution sway. With client desires for the cloud to give immediate access to cloud assets, it can be an extreme offer as an IT administrator, to strike a balance between cloud optimal performances with the necessity for secure information.

When to Encrypt Data

Ordinarily information do not stay in one spot on one's system, and this is particularly valid for information in the cloud. Scramble your data wherever it is in the cloud: very still, in procedure, or in movement.

Data in movement

- Data in flight over system on network (Internet, e-business, cell phones, ATM machine, etc.)
- Data that utilize communication protocols such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), Internet Protocol Security (IPsec), Hypertext Transfer Protocol Secure (HTTPS), FTP, and Secure Shell (SSH)

Data in procedure

- Transactional information in real time, or touchy personal financial information stored as scrambled fields, records, rows, or column data in a database
-

Data at time-out

- Files on personal computers, servers, and removable media
- Data stored using full disk encryption (FDE) and application-level models

B Secure Your Platform

Rootkit and other low-level malware assaults are expanding. They are hard to identify with conventional antivirus software's and use different techniques to stay undetected. Rootkit assaults contaminate system software components for example hypervisors, BIOS, and operating systems, and can cover up malware that works out of sight and spreads all through a cloud platform, bringing on expanding harm after some time.

With complex dangers and malware a continuous and developing risk, securing both customer and server platforms give an extra authorization point between servers and between servers and customers.

The most ideal approach to empower a trusted platform is to begin with a hardware-based root of trust and augment the chain of trust through the sensitive controlling software layers such as firmware, BIOS, and hypervisor virtualization layers. A foundation of trust solidifies the platform against assault and is greatly hard to crush or subvert. It significantly lessens the security dangers of utilizing a remote or virtualized framework and empowers a more secure platform for incorporate occupants and workloads. Basically one incorporates security into one's hardware to better protect one's software. A foundation of trust guarantees system integrity inside of every system. Integrity checking is considered a key ability for software, platform, and infrastructure security [16].

C Extend Trust across Federated Clouds

As cloud computing advances, the purpose of federated cloud relationships—crosswire which end-users, data, and services can move effortlessly inside and over a few cloud framework—adds another layer of intricacy to our security paradigm. Trusted access to the cloud and across clouds depend on overseeing characters and access-administration principles based single sign-on (SSO), solid verification, account provisioning, Application Program Interface (API) security, and audit functionalities. For cloud security, basic client usernames and passwords are no more sufficient in line of the fact that they can be effortlessly accessed. Secure SSO in light of solid extended verification is important in federated cloud platforms, where the cloud service provider is depending on the verification and authentication done by the enterprise to concede access to applications.

D Choose the Right Cloud Service Provider

Choosing a cloud service provider is confounded on numerous levels—from the cloud conveyance model and architecture to particular applications. To worsen matters, a few organization offer software as well as hardware and services. Moreover, one must be careful about ensuring the security one need to secure one's information and infrastructure are part of the services offer by the cloud provider. At the apex level, one needs to know whether the cloud provider or supplier can give confirmation of information and infrastructure securities they give. Once the criteria have been met, one can then build up quantifiable, enforceable Service Level Agreements (SLAs) to give continuous verification and authentication.

A rundown of extra security contemplations to consider while choosing a cloud service provider appears in table 1 [17].

Table 1: Cloud service security consideration

Security Selection Criteria	Consideration
Data center risk management and security practices	• What are the patch management policies and procedures? • How does technology architecture and infrastructure impact the cloud service provider's ability to meet SLAs?
Hardware-based security	• Can the cloud service provider offer trusted pools for the most sensitive workload? • Is encryption a software-only solution?
Technology segmentation	• How are systems, data, networks, management, provisioning, and personnel segmented? • Are the controls segregating each layer of the infrastructure properly integrated so they do not interfere with each other? For example, investigate whether the storage compartmentalization can easily be bypassed by management tools or poor key management. • What cloud access and identity protocols are used?
Identity and Access Management	• How is identity managed and authenticated? • Is two-factor authentication utilized?
Attack Response and Recovery	• How are attacks monitored and documented? • How quickly can the cloud service provider respond? • What recovery methods are used?
System Availability and Performance	• Is the cloud service provider financially stable? • How long has the vendor been in business? • What is their current financial standing?
Vendor Financial Stability	• Is the cloud service provider financially stable? • How long has the vendor been in business? • What is their current financial standing?
Product Long-term Strategy	• What is the vision for the service provider's cloud offering? • Does the cloud service provider have a product roadmap for their offering? • Cloud service providers seeking to provide mission-critical services should embrace the International Organization for Standardization/International Electro-technical commission (ISO/IEC) 27001 standard for information security management systems. • If the provider has not achieved ISO/IEC 27001 certification, they should demonstrate alignment with ISO 27002 practices.
Limits of Responsibility	• What is the limit of the cloud service provider's responsibility for security? • What security responsibilities are expected of the enterprise? • What is the legal accountability in a breach?
Compliance Capabilities	• Does the cloud service provider have the ability to comply with regulatory requirements that you face? • Is the cloud service

V. CONCLUSION AND FUTURE WORK

Frankly speaking, putting data and running software on another person's hard disk utilizing another person's Central Processing Unit (CPU) seems overwhelming to the general populace at large. This paper has looked into the security challenges facing cloud computing and plausible approaches to countermeasure them. Security issues in resource multi-tenancy, private data multi-location, cookie poisoning and privacy of data has been discussed. With various encryption techniques, platform security measures, extending trust across federated clouds and choosing the right cloud service provider these problems are grossly minimized. As no computer system can provide absolute security under all conditions more research is needed to investigate ways of curbing these security threats inherent in cloud computing.

REFERENCES

1. Rosado D,G, Gómez R, Mellado D, Fernández-Medina E. ' Security analysis in the migration to cloud environments. Future Internet 4(2):469–487, 2012
2. Zha G., Liu J., Tang Y., Sun W., Zhang F., Ye X., Tang N., Cloud Computing: A statistics aspect of users, First International conference on cloud computing (Cloudcom), Beijing, China, Springer Berlin, Heidelberg, pp 347-358, 2009
3. Mather T, Kumaraswamy S, Latif S. Cloud Security and Privacy. O'Reilly Media, Inc., Sebastopol, CA. 2009
4. Kresimir P. and Zeljko H. "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, pp. 344-349, 2010
5. Subashini S. and Kavitha V. "A survey on security issues in service delivery models of cloud computing." J Network Comput Appldoi:10.1016/j.jnca.2010.07.006, 2010.
6. Cloud Security Alliance (CSA). Available: http://www.cloudsecurityalliance.org, retrieved 2015
7. Kevin Hamlen, Murat Kuntarciogh, Latifur Khan, Bhavani Thuraisingham ,"Security Issues for Cloud Computing", International Journal of Information Security and, April-June. University of Texas at Dallas, USA. Privacy, 4(2),39-51, 2010
8. Srinivasa Rao V., Nageswara Rao N. K., E Kusuma Kumari," Cloud Computing: An Overview", Journal of Theoretical and Applied Information Technology www.jatit.org. 2005 - 2009
9. Arnold S. "Cloud computing and the issue of privacy" *KM World*,. Available: www.kmworld.com, pp14- 22 , 2009.
10. Kuyoro S. O., Ibikunle F. & Awodele O., "Cloud computing security issues and challenges", International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011
11. A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." *Platform Computing*, pp6, 2010.
12. Toyin Ogunmefun's Space," Effective Data Protection for Cloud Computing and its Relevance in the Nigeria Economy".Available: http://toyinogunmefun.wordpress.com June 18, 2015
13. Drue Reeves (2009),"Cloud Computing: Transforming IT", December 3rd, 2009. Available at: http://net.educause.edu/ir/library/pdf/ECRC0901.18, 2015
14. Vahid Ashktorab, Seyed Reza Taghizadeh," Security Threats and Countermeasures in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM) Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com, volume 1, Issue 2, October ,2012
15. Albert B Jeng, Chien Chen Tseng, Der-Feng Tseng, Jiunn-Chin Wang, "A Study of CAPTCHA and its Application to User Authentication", Proc. Of 2nd Intl. Conference on Computational Collective Intelligence: Technologies and Applications, 2010.
16. IntelITCenter "cloud computing security planning guide", available from Intel.com/ITCENTER Accessed 26th September, 2013
17. Adapted and expanded from *How to Choose a Cloud Computing Vendor*. how-to-choose-a-cloud-computing-vendor.html, Inc.com). inc.com/guides/2010/11/, November 29, 2010

BIOGRAPHY

Ejem Agbaeze is an Assistant lecturer in Computer Science Department, Federal University of Technology, Owerri, Imo State, Nigeria. He had is Master degree in Computer Science in 2015, from Federal University of Technology, Owerri, Imo State, Nigeria. His research interests are Cloud Computing, Simulation and Modelling and Software Development.

Dr. Nwokorie E.C., is a Senior lecturer in Computer Science Department, Federal University of Technology, Owerri, Imo State, Nigeria. She had her Doctorate degree in Computer Science in 2015, from University of Port Harcourt, River State, Nigeria. Her research interests are Database, Operating System, Data Communication, Simulation and Modelling etc.

Njoku Donatus is a Ph.D student in Computer Science Department, Federal University of Technology, Owerri, Imo State, Nigeria. He had his Master degree in Computer Science in 2016, from Federal University of Technology, Owerri, Imo State, Nigeria. His research interests are Database, Embedded Systems, and Software Development.

Dr. Odii J.N., is a Senior Lecturer in Computer Science Department, Federal University of Technology, Owerri, Imo State, Nigeria. She had her Doctorate degree in Computer Science in 2016, from Nnamdi Azikwe University, Awka, Anambra, Nigeria. Her research interests are Data Communication and Networking, Mobile Communication.

Adibe Francisca is an Assistant lecturer in Computer Science Department, Federal University of Technology, Owerri, Imo State, Nigeria. She her Master degree in Computer Science in 2016, from Federal University of Technology, Owerri, Imo State, Nigeria. Her research interests are Data Communication and Networking, Simulation and Modelling and Software Development.