Mitigating Malicious Software Threat in Cloud Computing Models Using-Multi-Factor-Authentication-in-Cloud-Computing

Oguji Francis Chikezie., Amanze B.C., Agbakwuru O.A & Agbasonu V.C
Department of Computer Science, Imo State University, Owerri
amanzebethran@yahoo.com

DOI: 10.56201/ijcsmt.v9.no5.2023.pg139.149

Abstract

This paper mitigating malicious software threat in the cloud computing models is on securing cloud computing platforms. Cloud storage providers store the data in multiple servers maintained by hosting companies. This increases the risk of unauthorized access to the private data. Even though the cloud continues to gain popularity in usability and attraction, the problems lies with data confidentiality, loss of control, lack of trust, data theft and the fact that user data is stored in unencrypted format. This can subject the data to malicious software threats. This paper focuses on malicious software threats presented by cloud service providers. Using encryption techniques and intrusion detection system, the risk of unauthorized access can be controlled. In the proposed methodology, a user encrypts files with secret keys before uploading them into the cloud. Once encrypted, the file is stored in an encrypted format in the cloud. For a user to download files form the cloud, the file owner first accepts a request by an authorized user, and an application server provides an Access key. Using an access key, a user downloads data and uses a secret key to convert cipher text into a plain text. This technique ensures end-to-end encryption and completely hides the data from cloud service providers hence maintain confidentiality. Implementation involved building an encryption application algorithm, for deployment on the user computer. The system is simulated using a web-system developed with PHP, MySQL and JavaScript. The System design followed the OODM methodology. The software performance was tested using speed of data retrieval and security of the data protection. The security looks at the ability of the system to determine fraudulent users and deny them access to the system. The result obtained from the new system developed shows a high level of data security level as compare to existing system that uses only password for authentication.

Keywords: *Multi-factor authentication, Cloud computing Platforms, Data Protection and Software Threats.*

1.0 Introduction

Cloud computing is the evolution of an existing information technology (IT) infrastructure that provides a long-dreamed vision of computing as a utility. The emergence of cloud technologies over last several years had significant impacts on many aspects of IT business. According to the survey conducted about cloud computing, most of medium and small companies use cloud computing services due to various reasons, which include reduction of cost in infrastructure and fast access to their application [1]. Cloud computing has been described in terms of its delivery and deployment models. Although cloud computing emerges from existing technologies, its computing (delivery and deployment) models and characteristics raise new security challenges due to some incompatibility issues with existing security solutions [2]. Cloud computing includes a group of computers that are jointly used to provide different computations and tasks. One of the key benefits that is offered from this IT technology for the companies is reduced time and costs on the market. Cloud computing is providing companies and organizations to use shared storage and computing resources. It is better than to develop and operate with the own infrastructure. Cloud computing also provides organizations and companies to have a flexible, secure, and cost-effective IT infrastructure. Main corporations including Google, Amazon, Cisco, IBM, Sun, Dell, Intel, HP, Oracle, and Novell have invested in cloud computing and propose a range of cloud-based solutions to individuals and businesses. There are different types and models in cloud computing regarding the different provided services. Cloud computing could be usually classified by two ways: by cloud computing location, and by the offered types of services. By the location of the cloud, cloud computing is typically classified in: public cloud (where the computing infrastructure is hosted by the cloud vendor); private cloud (where the computing infrastructure is assigned to a specific organization and not shared with other organizations); hybrid cloud (the usage of private and public clouds together); and community cloud (it involves sharing of IT infrastructure in between organizations of the same community), [3]. If the classification is based on type of offered services, clouds are classified in these ways: IaaS (Infrastructure as a service), PaaS (Platform as a Service), and Software as a Service (SaaS) [3]. When we utilize cloud computing we run our software on hard disks and CPUs that are not in front of us. That is why users are having more doubts about the security issues when they are using this technology. So, a lot of different types of attacks could happen in the cloud technology. Besides the above mentioned, most known attacks involve phishing, IP spoofing, message modification, traffic analysis, IP ports, etc. There are a lot of security techniques for data protection that are accepted from the cloud computing providers, and they all provide authentication, confidentiality, access control and authorization. The problem of software security has taken a new dimension in recent years. Attackers now followed a specialized method, for exploiting security hole contain in deployed software applications and launch malicious attacks on target software in real-time, before software developer become aware of the vulnerability or distribute patches for security fix. This method is known as Zero-Day exploits, and the term is deriving from the age in which the attack occurs before the security holes are either became known to the developer or being provided a solution. They come in the form of Zero-day malware, scanning worm, software injection, buffer overrun and to mention but a few [4]. In cloud computing, this prevalent malicious software attacks due to software vulnerabilities are perceived as big challenge particular as the future of cloud computing is yet uncertain [5]. Many cloud customers still doubt the uncertainty and readiness to be able to guarantee and secure huge data which are to be deployed and host on the net. Malicious software, or malware for short, is software designed with a nefarious intent of harming the computer user. There are many types of malware, depending on how they are spread and the nature of harm they intend. Some examples of malware include – viruses, worms, Trojan horses, spyware, keyloggers, botnets, rootkits, ransomware, scareware, and drive-by downloads. To date, over a million different viruses and other malware have been detected. Malware can be prevented by using appropriate security software such as firewalls, antivirus software, and antispyware. In addition, researchers have employed criminological theories, in particular, self-control and routine activity theories, to determine factors that may increase the risks of malware infection victimization. The extant evidence indicates that irresponsible use of the Internet, such as failing to use security software or clicking on questionable websites, can also lead to malware infection victimization. Accordingly, to effectively address malware, the technical aspects of the problem as well as the human side of the issue must be jointly considered and targeted. Malware developers are getting smarter in terms of their ability to develop malware that goes undetected by antimalware software, and antimalware developers need to constantly remain innovative to combat smarter malware.

2.0 Review of Related Works

Table 1: Related works

Author	Techniques	Work done	Limitations
[6]	Encryption algorithm	Focused on authentication, stronger and faster encryption algorithm, and file integrity	Introduced delay in data transmission
[7]	Multi factor Authentication	systematic method for authenticating clients, namely by using a password, biometric, and out-of-band-based access control mechanisms that are suitable for access control	Depends on several factors, such as the lack of availability of the mobile network, which can cause a delay in obtaining the OTP
[8]	OTP technique	Improved authentication system	Didn't consider network availability which can lead to failure
[9]	multiplayer system	protection against DDoS in the cloud	pointed out that no standalone technology today would stop a powerful DDoS reflection attack over 500 Gb/s
[10]	Multi-Authority Authentication	created different authentication mechanisms	Lacks effective access control
[11]	Biometric	reduction of cost and ubiquitous access	The key for salting the encryption is user dependent

[12]	Multi-tier Authentication Technique	With number of authentication tiers in the system, the probability of success for breaking the multi-tier authentication system reaches near to the zero	The technique takes more space
[13]	Predicate Based Encryption (PBE)	permits a single encrypt or/multi decrypt or environment to be realized using a single scheme	precludes unwanted exposure, unwanted leakage and other unwanted breaches of confidentiality of cloud resident data
[14]	Secure Authentication	Supports device and user authentication service and the confidentiality and integrity can provided	provide very low authentication and security services
[15]	Cryptographic with biometric features	Improved the security for sensitive data	The problem with this feature is the impossibility of sharing the encrypted data with another remote user
[16]	Fine-grained Two-factor Access Control	Achieved the desired security requirements	Low efficiency
[17]	Digital Signatures	Better performance	High Cost of implementation
[18]	combined algorithm (AES, RSA and SHA2)	data security framework is secured	The system didn't cover Card validation process, customer identification process
[19]	Attribute Based Encryption	keeps the character spillage and accomplish the full secrecy	No implementation done
[20]	Biometric-based Authentication	Improved cloud security	Requires the use of additional hardware to support the functioning of an authentication
[21]	Transparent Biometric Cryptography	enhanced the security and usability issues of cloud storage technology	Limited scope of study
[22]	Device fingerprinting	dual- authentication process targeted at authenticating the device and the user	cost from fingerprinting all devices will be very high
[23]	two-factor authentication	increase the security of the cloud environment	two factor authentications still have loop holes for security breaches

[24]	Mobile One Time Passwords and RC4 Encryption	the user's mobile phone that provide the passwords, and that the whole solution is based on open source code	the time synchronization between the phone and server should be fixed
[25]	OTP	ensures protection against eavesdropper's attack and man-in-middle attack	Needs improvement
[26]	OTP	Prevented attacks like brute force attack, phishing, Distributed Denial of Service (DDOS) through password encryption	Needs improvement
[27]	multi factor authentication scheme	multi factor authentication scheme implementing a PIN, OTP, and biometric fifingerprint	data in transit and storage should be protected using end-to-end encryption
[28]	Third Party Auditor	They use encryption to ensuring the data integrity	higher resources cost
[29]	Authentication and Encryption	focus is on client-side security in which only the authorized user can access the data	Didn't cover the security at both ends
[30]	OTP based data security model incorporating AES and SHA2	reduced the complexity, processing cost which increases the overall efficiency of the system	failed to inculcate identity management in the system
[31]	encryption techniques	A user encrypts files with secret keys before uploading them into the cloud	Requires maintenance of many secret and private keys

3.0 Methodology/ Analysis

Object-oriented analysis and design methodology (OOADM) was adopted in this research work and it is a set of standards for system analysis and application design. It uses a formal methodical approach to the analysis and design of information system. Object-oriented design (OOD) elaborates the analysis models to produce implementation specifications. The main difference between object-oriented analysis and other forms of analysis is that by the object-oriented approach we organize requirements around objects, which integrate both behaviors (processes) and states (data) modeled after real world objects that the system interacts with. This paper proposed Multi-Factor-Authentication-in-Cloud-Computing that will involve user ID/password, Advanced Encryption Standard (AES), and Digital Signature for Intrusion Detection System (IDS) for verifying the intended user to overcome the malicious software threats and providing single-sign on access of the registered services. The proposed authentication technique works on two phases. In the first phase, the users register themselves with the first-tier and second-tier authentication credentials. For the second-tier authentication, the user does not need to provide the authentication credentials like first-tier and second-tier authentication. The system is using the mobile secret code as the third-tier authentication code (One Time Password – OTP). This secret code is valid for some amount of time to access the requested service. One provides the time limit with the secret code. After the time limit expires, the user cannot access the requested service with that secret code. The user needs another secret code for accessing the requested service. The proposed scheme follows the following steps to authenticate the user for accessing the requested services.

1. For accessing the services, the user provides the URL of the cloud service provider in the web browser which sends the request to the cloud server for loading the Login GUI of the cloud service provider.
2. The user provides the registered username and password (first-tier authentication credentials) at the login GUI for verifying themselves to the cloud server.
3. If the username and password provided by the user to the cloud server is correct, then the cloud server sends the reply of validation at the user side. The application program or observer gets this validation reply at the user side.
4. Once the user enters the password and submits this information to the application program, the system extracts his/her phone number from database and sends the secret code (OTP) on the registered contact number of the user. This secret code has some time limit which is set by the cloud service provider. After the time limit, the code will be expired and no more use of that code.
5. The users provide the OTP which they got on their mobile number to the secret code submission screen for authenticating themselves.
6. Once the user provides the secret code to the system, it will match the code which it sends to the user and also checks the time limit of that code. If the user provides the correct secret code within the time limit, then the system initiates the code for loading the requested service in the web browser.
7. After initiating the code of requested service, the observer loads the requested service in the user’s web browser.
8. Once the requested service is loaded into the web browser of the user, direct communication has been established between the user’s web browser and the cloud server.

Once access is granted to the user, all data transmission will be encrypted using Advanced Encryption Standard (AES). AES is an iterative instead of Feistel cipher. It is based on two common techniques to encrypt and decrypt data known as substitution and permutation network (SPN). SPN is a number of mathematical operations that are carried out in block cipher algorithms. AES has the ability to deal with 128 bits (16 bytes) as a fixed plaintext block size. These 16 bytes are represented in 4x4 matrix and AES operates on a matrix of bytes. In addition, another crucial feature in AES is number of rounds. The number of rounds is relied on the length of key. There are three different key sizes are used by AES algorithm to encrypt and decrypt data such as (128, 192 or 256 bits). The key sizes decide to the number of rounds such as AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. In this thesis, 128 bits AES algorithm was used and it uses a particular structure to encrypt data to provide the best security. Also, the paper proposed to improve data transmission security in wireless data network wireless using digital signature. Digital signature is the one of the verification technique. The certification process in an asymmetric key algorithm depends on digital signatures to provide trust. A digital signature is an electronic method of signing an electronic document that is reliable, convenient and secure. A digital signature mechanism consists of a digital signature generation and associated digital signature verification. A simplistic model of digital signature schemes involves a sign operation that uses a sender's private key to generate a signature. The receiver retrieves the sender's certified public key from a Certificate Authority (CA) and performs a verify operation on the signature. A successful verification procedure convinces the receiver that the received message is from the actual originator and the contents are not tampered since leaving the originator.

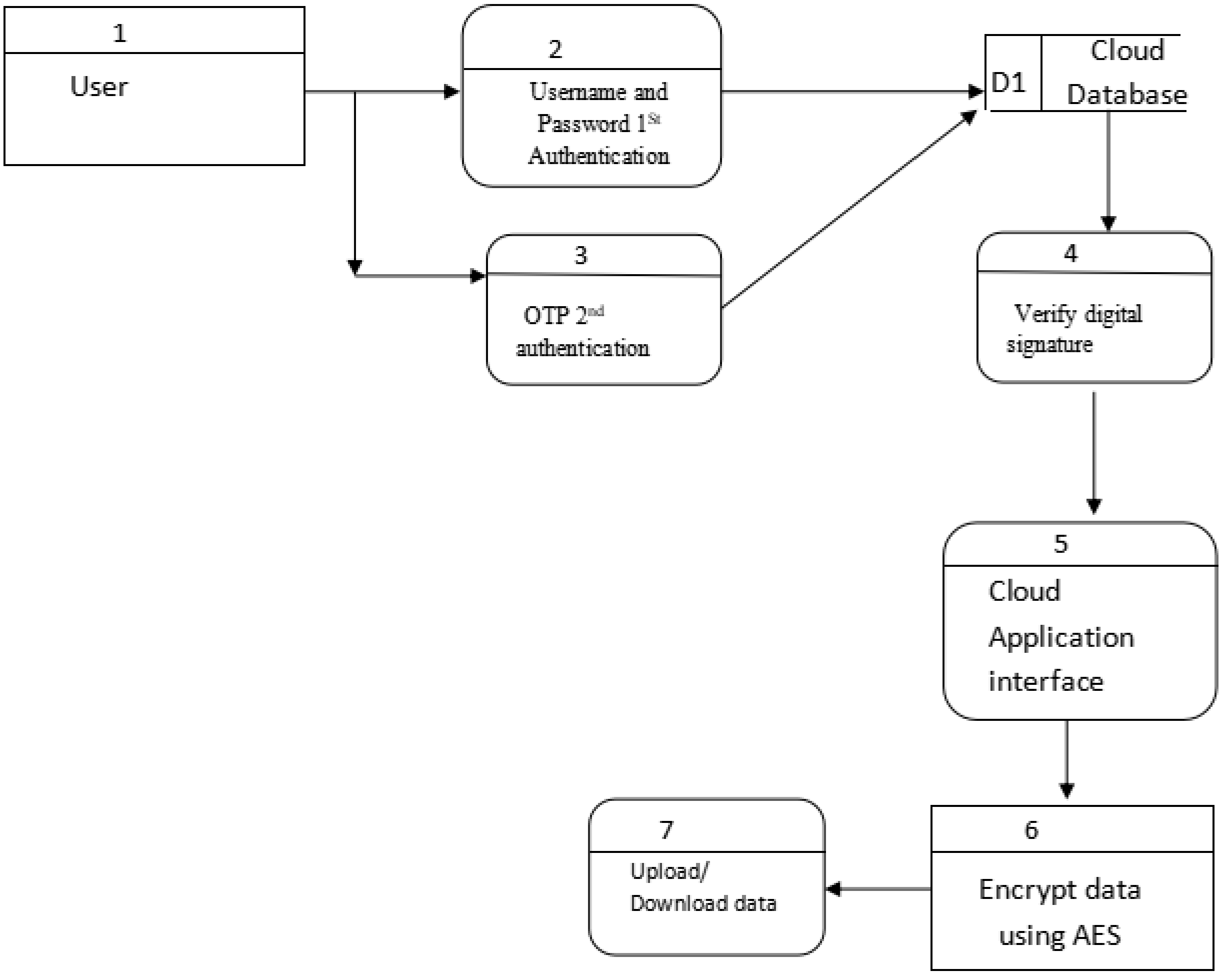

Figure 1: **Data Flow Diagram (DFD) of the Proposed System**

Figure 1 shows Data Flow Diagram for the model showing the flow of process between the components. The user is first verified using password and OTP. Then the digital signature of the device is verified. A file is encrypted at the user computer before upload. Whenever the user uploads a file, the encryption algorithm will generate a secret key. A secret key is generated during encryption of a file. The key is used for both encryption and decryption. A user needs an access key to access a file from the cloud.

4.0 Performance Evaluation

The software performance was tested using speed of data retrieval and security of the data protection. The security looks at the ability of the system to determine fraudulent users and deny them access to the system. The speed and security level obtained is as presented in the table below.

Table 2: **Performance Results Obtained**

Technique Applied	Security Level	Speed
Cloud Database	97%	100Mb/s

Conclusion

Cloud based system faces a lot of security concerns and this scares organizations away from hosting their database in the cloud environment. Most security concerns centers on the privacy and validity of their data. This calls for more secured authentication system for cloud computing. Any authentication system’s core strength depends upon the probability of success for breaking that system for accessing the services provided by the cloud service providers. In this thesis authentication scheme, the core strength is first-tier, second-tier and third-tier authentication user credentials. For getting the access of the requested service, the attacker has to break all the authentication layers. At the first tier, the username and password of the user is verified. At the second tier, OTP is sent to the user’s phone number and the user is expected to enter the OTP for final identification. Security analysis says that increases as the number of authentication tiers in the system, the probability of success for breaking the multi-tier authentication system reaches near to the zero. Hence, looking at the security model used in this thesis, one can say that there is a very less probability of breaking the multi-tier authentication system. Also, the AES algorithm was used to secure the data more by encrypting the data stored in the cloud-based database. With the above security measures, the data security in the cloud is guaranteed and it will encourage people to use cloud-based systems as the security of data is guaranteed.

References

[1]. Subashini, S. and Kavitha, V. (2018). A Survey on Security Minimal issues in service delivery models of cloud computing Journal of Network and Computer Applications, 34(1), 1- 11

[2]. Kaufman, L. M. (2020). Can public-cloud security meet its unique challenges? Security & Privacy, IEEE 8.4 (2020): 55-57

[3]. Badger, L., Grance, T., Patt-Corner, R. and Voas, J. (2015). Cloud computing synopsis and recommendations (draft), nist special publication 800-146, Recommendations of the National Institute of Standards and Technology, Tech. Rep.

[4]. Dunlop, M.; Groat, S.; Shelly, D. (2020). GoldPhish: Using Images for Content-Based Phishing Analysis, Internet Monitoring and Protection (ICIMP), 2020 Fifth International Conference, pp.123-128, May 2020.

[5]. Jun, F.; Yu, C.; Wei-Shinn, K.; Pu, L. (2019). Analysis of Integrity Vulnerabilities and a Non-repudiation Protocol for Cloud Data Storage Platforms, Parallel Processing Workshops (ICPPW), 2019 39th International Conference, pp.251-258, Sept. 2019.

[6]. Eman, M. M., Hatem, S. A. and Sherif, E. (2013). Data Security Model for Cloud Computing. Department of Computer Science, Faculty of Computers and Information, Menofia University, Menofia 32511, Egypt

[7]. Subhash, C. P., Sumit, J., Ravi, S. S., and Jyoti, C. (2018). Access Control Framework Using MultiFactor Authentication in Cloud Computing. International Journal of Green Computing Volume 9 • Issue 2 • July-December 2018

[8] .Mohanaad, S. and Aaisha, K. (2019). Improving Authentication system for public cloud Computing. publication at: https://www.researchgate.net/publication/331035798

[9]. Badr, A. (2016). Proactive Approach for the Prevention of DDoS Attacks in Cloud Computing Environments. A dissertation submitted to the School of Computing at Florida Institute of Technology.

[10]. Nayyar, M. A. (2016). Multi-Authority Authentication System for Cloud Data Storage. Computer Science and Engineering Department Indian Institute of Technology, Kharagpur Kharagpur – 721302

[11]. Agbasonu, V. C. (2017). Cloud computing security for data at rest and data on transit. International Journal of Scientific Research and Innovative Technology ISSN: 2313-3759 Vol. 4 No. 2; February 2017

[12]. Munjpara, P. P. (2018). Implementation of Multi-tier Authentication Technique for Single-Sign On access of Cloud Services. Department of Computer Science and Engineering National Institute of Technology, Rourkela Rourkela-769 008, Odisha, India

[13]. Muijnck-Hughes, J. (2019). Data Protection in the Cloud, 12 Jan, 2019 [Online], Available: http://www.ru.nl/ds.

[14]. Jin-Mook, K. and Jeong-Kyung, M. (2014). Secure Authentication System for Hybrid Cloud Service in Mobile Communication Environments. Division of Information Technology Education, Sun Moon University, No.100 Galsan-ri,Tangjeong-myeon, Chungnam.Asan-si336708,RepublicofKorea

[15]. Ivana, K. (2016). Cloud security - An approach with modern cryptographic solutions. Computer Science Department, Indiana University, Bloomington IN 47405

[16]. Joseph,K., Liu, M., Xinyi, H., Rongxing, L., Jin, L. (2020). Fine-grained Two-factor Access Control for Web-based Cloud Computing Services

[17]. Gowtham, N., Kumar, K., Praveen, K. R. (2014). Hash Based Approach for Providing Privacy and Integrity in Cloud Data Storage using Digital Signatures. N Gowtham Kumar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 8074-8078

[18]. Edil, E. (2016). Cloud Data Security Framework for Paym ent Card System: the case of Ethiopia. A Thesis Submitted to the Department of Computer Science in Partial Fulfillment for the Degree of Master of Science in Computer Science Addis Ababa, Ethiopia.

[19]. Anirudh, M. (2017). Attribute Based Encryption for Secure Data Access in Cloud. Culminating Projects in Information Assurance. 39. https://repository.stcloudstate.edu/msia_etds/39

[20]. Asmaa, M. H. (2018). Biometric-based Authentication Techniques for Securing Cloud Computing Data. International Journal of Computer Applications (0975 – 8887) Volume 179 – No.23, February 2018

[21]. Leith, H. A. (2019). Securing Cloud Storage by Transparent Biometric Cryptography. University of Plymouth, https://pearl.plymouth.ac.uk

[22]. Paul, E. M. (2016). Device fingerprinting identification and authentication: A two-fold use in multi-factor access control schemes. Graduate Thesis and Dissertations. 15968. https://lib.dr.iastate.edu/etd/15968

[23]. Vishal, P., Vimmi, P. (2013). An Improved Authentication Technique with OTP in Cloud Computing. International Journal of Journal Scientific Research in Computer Science and Engineering. Research Paper Vol-1, Issue-3 E-ISSN: 2320-7639

[24]. Markus, J. and Faruque, A. (2015). Mobile One Time Passwords and RC4 Encryption for Cloud Computing. School of Information Science, Computer and Electrical Engineering Halmstad Universit

[25]. Pandey, V. (2017). Securing the Cloud Environment Using OTP. International Journal of Scientific Research in Computer Science and Engineering

[26]. Niharika ,G. and Rama, R. (2015). Implementing High Grade Security in Cloud Application using Multifactor Authentication and Cryptography. International Journal of Web & Semantic Technology (IJWesT) Vol.6, No.2, April 2015

[27]. Guma, A., Mussa, A. D. and Anael, E.S. (2020). Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures. Future Internet 2020, 12, 160; doi:10.3390/fi12100160 www.mdpi.com/journal/futureinternet

[28]. Bhavna, M., V. G. (2013). Enhanced Data Security in Cloud Computing with Third Party Audito. International Journal of Advanced Research in Computer Science and Software Engineering, pp 341-345.

[29]. Sanjoli, S., J. S. (2018). Cloud Data Security using Authentication and Encryption Technique. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2018, pp 2232-2235

[30]. Jaspreet, K., Navdeep, K. (2018). An OTP based data security model incorporating AES and SHA2 in cloud environment. International journal of Computers and Technology, Volume 17 Number 1, ISSN 2277 - 3061

[31]. Mwanyika, J. M. (2017). Confidentiality Protection Model for Securing Data In Cloud Computing. Degree of Master of Science in Information Technology at Strathmore University Faculty of Information Technology Strathmore University Nairobi, Kenya