Security of Cloud Storage System using Various Cryptographic Techniques

Abid Hussain [#1],Chungen Xu*[2], Muqadar Ali [#3]
[1,2,3] *Department of Mathematics, Nanjing University of Science and Technology Nanjing, China*

Abstract

Cloud computing platform is providing opportunity for sharing resources, information's and services among the users of entire world. Existence of huge secret data on the cloud. The security of cloud becomes a biggest concern for researcher's, malicious activities are growing with the growth of user in the cloud. Millions of peoples are using cloud for various purpose, that's why they need more secure and persistent services. In this paper we have purposed new security architecture for cloud computing platform. This ensures more secured communication system and protect your data from attackers. AES based file encryption system and asynchonous key system for exchanging data or information is incorporated into our model. Our proposed structure can be applied with main cloud computing features, e. g, SaaS, IaaS, PaaS. We include OTP (one-time password) system for user authentication ECC (Elliptic curve cryptography) has been proposed in this model for safe communication between client and cloud storage system. Our work primarily deals with the Security system of the whole cloud computing platform.

Keywords: *Cloud computing, Security architecture, AES, ECC, Onetime password, SHA2 Hashing.*

I. INTRODUCTION

At the existing world of networking system, one of the most significant and emerging concept for both users and developer is cloud computing [1]. Cloud computing is better platform for those who are interrelated with the networking environment of the current world. Consequently, Security has become a big challenging problem in cloud computing. In the cloud setting resources are shared between all the servers, users and individuals. As the outcome data or files kept in the cloud become open to all. Therefore, files or data of an individual can be handled by all other cloud users [2,3]. As a result, an intruder can easily access, destroy and misuse the original form of data. And also, can interrupt the communication. Besides, cloud service provider(CSP) provide distinct type of applications which are of very critical nature. For this it is also much vital for the cloud to be secure. [4] Another issue with cloud is that an individual might not have control over the place where the data have to be stored. Since a cloud consumer got to utilize the resource allocation and planning provided by the cloud service provider. For this it is additionally important to ensure the data or files amidst unsecured procedures. With a specific end goal to tackle this issue we have to apply security in cloud computing platform. In our proposed security structure, we have tried to take into security of account breaches as much as possible. At present many security algorithms and model are applied within the area of cloud computing. But unfortunately, these models have failed to resolve all security threats. [5,6,7] Furthermore for various kinds of online business and E-commerce [8] we need to imply high capability security model in cloud computing fields. Security models that are produced and presently utilized as a part of the cloud computing environment are basically utilized for giving security to a file and not for the entire communication system [9]. Additionally, present security models are in some cases utilizing secured channel for communication [10] But this is not cost-effective process. Again, it's rare to search out a combined work of main server security, transection between them and then on. A few models however Endeavor to talk about these, they are completely subject to client approach and neglected to utilize machine intelligence for generating key and newer proposed model. Some models have worked with reference to hardwire encoding system for secured communication system. [11]. It is straightforward to assume however terribly tough to implement. Besides, hardwire encryption is useful just for database system, not for other security issues. Again, authenticated user detection is now a day very important thing, which is infrequently discussed in that models which is used to ensuring the security in the cloud computing

The main contributions of this paper are summarized as follow:

In this paper demonstrate a newer security architecture for cloud computing platform. Where files are encrypted using cryptographic algorithm AES in which keys are generated randomly by the system. One key is generated for only one file. we have used distributed server concepts here for ensuring high security. The proposed model additionally helps to resolve key security problems like intruders, malevolent, hacking etc. of cloud computing platform. We used ECC algorithms for Secured communication between the server's and users.

The rest of paper is structured as follow, section II discuss related works to cloud computing architectures and models; In section III we present our proposed cloud computing architecture, Section IV describe the execution process of proposed architecture; section V discuss the experimental and graphical result of proposed architecture; section VI discuss about the advantages of proposed model and section VII discusses on our achievements and future works.

II. RELATED WORKS

Various research on cloud computing security have already completed in recent days Different researchers are discovered on Identification based mostly cloud computing security model [12]. But only detecting authentic user does not all the time obstruct data intruding or data hacking in the database of cloud environment. For secure data saving in cloud server Yao's Garbled circuit has use [13,14]. That is also identification based work. The weak point in this system is that it does not working to ensure the security in whole cloud computing platform Research regarding guaranteeing security in whole cloud computing environments was already figured out in numerous structures and formed. AES based file encryption system is employed in a number of these figured out models [15,16]. However, these models keep both the encryption key and encrypted file in one database server. A single successful malevolent attack in the server may exposed the whole information files to the hacker, which is not attractive. Some other models and architecture are also proposed for ensuring security in cloud computing environment [17,18]. while these models build safe communication among users and servers, but they don't encrypt the uploaded data. For best security making certain method, the uploaded data must be encrypted so nobody will get access to that data and its location.
Recently some others precious secured models for cloud computing environment are also researched out [19,20]. But, these models also fail to guarantee all conditions of cloud computing security subjects [21].

III. SYSTEM MODEL

We construct our model using the following security algorithms

- For secured file encryption we have use AES [22,23,24].
- For secured communication we used ECC.
- We used SHA2 hashing for cover the tables from user
- For user authentication we used Onetime password(OTP). [29,30]

Currently one of the most significant problem for researchers is become the security in cloud computing platform. We have worked about this problem in our research, to find solution associated with security.
We have proposed a security model for cloud computing data storage shown in Figure 1.
In this model, we can observe that all the User's need to communicate with the main server, and with the help of this System computer users can communicate easily with data bases for uploading or downloading their files. The system server helps the user every time. It takes files from the users, and keeps these files in different databases, which relates to system server, and retrieve files from the databases to Users whenever needed.

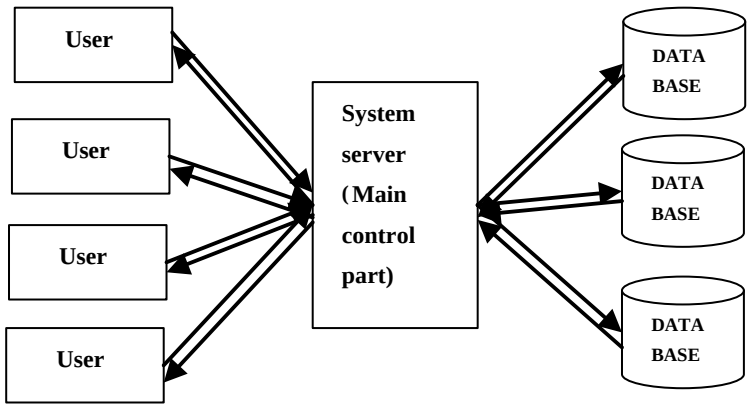

Figure 1. Proposed Security Model

We have worked with ECC for secure communication [25,26]. Usually the request of User's is encrypted while sending to the cloud service provider system. ECC encryption algorithm using the Public key of the system for the encryption. Whenever the User request to the system for a file then the system sends it by encrypting it via ECC encryption algorithm using User's public key. The similar procedure is also applied for the password requests. While logging in the system later. The user browser will decrypt the file with ECC

algorithm using user's private key after received an encrypted file from the system. Same process is also applied when system receives an encrypted file from the user it will decrypt it by its private key. The outcome, communication between user's and system become secured.

In our model we used the OTP (onetime password) for authentication of user [28,29,30]. The main purpose of using password is to make ensure the security and confidentiality of user account from malicious person. To control this problem, we used onetime password in this model. So whenever enter in the system He/she will be provided with a new password for using it in the next log in. Usually this is provided by the system itself and the password will be generated randomly. Each time a new password will provide for a user and the previous password will be removed from the system. New password will be updated for that user. A single password can be used only once time for log in. Password will be sent to that user's authentic mail account. consequently, at that time, a check to determine the user validity is also performed. As the output only, authorized users having valid mail account can be able to connect with cloud system. With this System, existence of unauthorized user or a user having invalid mail account will be noticed. After SHA2 hashing the new generated password is stored in the system [27]. The purpose of using SHA2 hashing is that this method is strong. So, it will be complicated for unauthorized or anonymous party to gain password for a selected user even if gained access to the system database. After connected with the system user will be able to upload or download the file. In the first time when user connected with the system can only upload file. There after users can perform both operation upload and download their files from the data storage. When a user uploaded a file the system server encrypts the file using AES encryption algorithm [28]. Our proposed model used 256 bits key for AES encryption.128 bit or 192 bits can also be used for this purpose. The system server has generated randomly 256 bits key here. A single key is used only once. That key is used for encrypting and decrypting a file of a user for that instance. This key cannot further have used in any instance later. The Key is kept along with the user account name in the data base table of the system server. SHA2 hashing hashed the user account name before inserting it. This ensure that any unauthorized party cannot recover the key to decrypt a specific file for a specific user by simply gaining access and observing the database table of the system server.

So as the outcome the key for a specific file become hidden and secured. Again, while encrypted file is uploaded for storing to the storage server, the user account along with the path of encrypted file is kept and preserve in the database table on the storage server. Whenever a user wants to download a previously stored file the Login in the system is compulsory for the user. When the user selects the file for downloading, the system retrieves the key for the requested file automatically from the main system. Then the system matches user account name saved in its database table with that saved in the storage server after hashing it using SHA2 hashing algorithm. The path of encrypted file from the storage server is found by using the account name of user and the hash table input for the requested file. In the proposed model encryption key for specific user is only known to the main system server, the path of encrypted file is known only the storage server which is known only to the main server. So, for this, the encrypted file and the key is hidden from malicious party. In this communication system when a file is sent to the storage server from the main system server it is in fully encrypted form. That's why to provide the security is not compulsory in this communication channel.

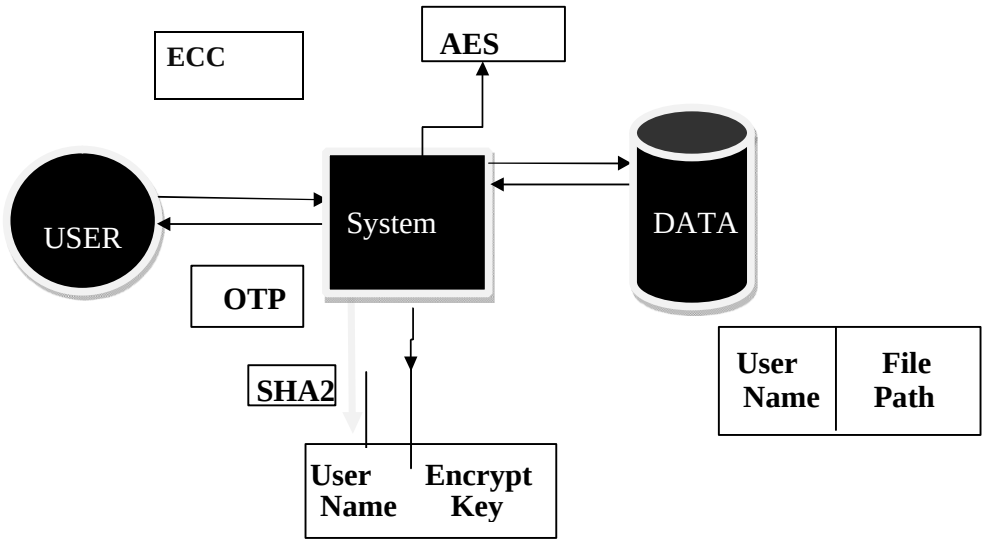

Figure 2. Proposed Security Model

Figure 2 is illustrating the proposed cloud security architecture. Here single user and server represent n user and n server.

IV. EXPREIMENTAL RESULT

In the lab we have worked with 70 users and also with their files for studying and prove the proficiency of the proposal model. We have tried to find out the result of different implementations which helped us to demonstrate our proposed model with better result. Various Condition and situations were observed while working and execution of this proposed model.

LAB SETUP:
Platform: Visual studio 2017(ASP.NET)
Processor: Intel(R)Core(TM)i3-4010U CPU@1.70GHZ.1.70GHZ
RAM:4.00GB
HD:374GB
Internet:1075kbps
System Type: 64.bit Operating System, x64-based processor
Windows edition: Window 8.1 Pro@2013 Micro soft corporation
Model: Haier Win.8.1PC
In this environment, the complete model took average of 5 second for executing whole steps. This model is sufficiently quick and can be applied to the current cloud computing environments.

IV. CASE STUDIES

Working with the model in the laboratory at various times and with totally different users and their individual files, which are not quite the same as each other in size, extension, contents, etc. take various times for executing the whole model. Depending on the file size, program execution time varies from in individual to individual. Among the 70 users result,10 of them are shown in table III and table IV.

TABLE III EXECUTION TIME FOR UPLOADING FILE OF 10 USERS

No of User	Size of File	Time Required for file Upload (Full Process)	No of User	Size of File	Time Required for file Upload (Full process)
1	1 KB	1.2 Sec	6	6 KB	5 Sec
2	2KB	1.8 Sec	7	7 KB	5.5 Sec
3	3 KB	2.7 Sec	8	8 KB	6 Sec
4	4 KB	3.2 Sec	9	9 KB	6.4 Sec
5	5 KB	4.3 Sec	10	10 KB	7.7 Sec

Table Iv Execution Time For Downloading File Of 10 User

No of User	Size of File	Time Required for File Download (Full Process)	No of User	Size of File	Time Required for file Download (Full Process)
1	1 KB	1 Sec	6	6 KB	4.7 Sec
2	2 KB	1.5 Sec	7	7 KB	5 Sec
3	3 KB	2.4 Sec	8	8 KB	5.6 Sec
4	4 KB	3 Sec	9	9 KB	6 Sec

5	5 KB	4 Sec	10	10 KB	7.1 Sec

GRAPHICLE RESULT: we have described simulation result with Uploading Phase in Fig .3 as shown below, while Downloading phase has been illustrate in Fig.4.

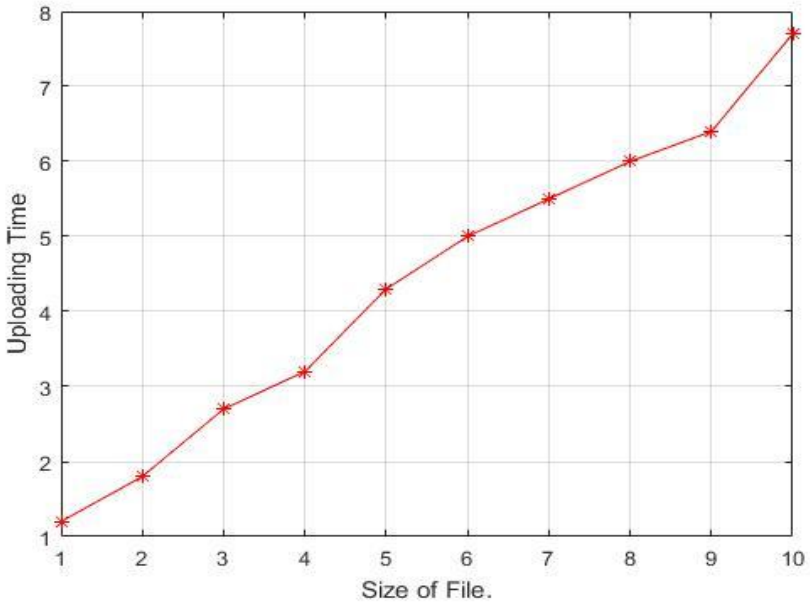

Fig: 3 Time Required for File Upload

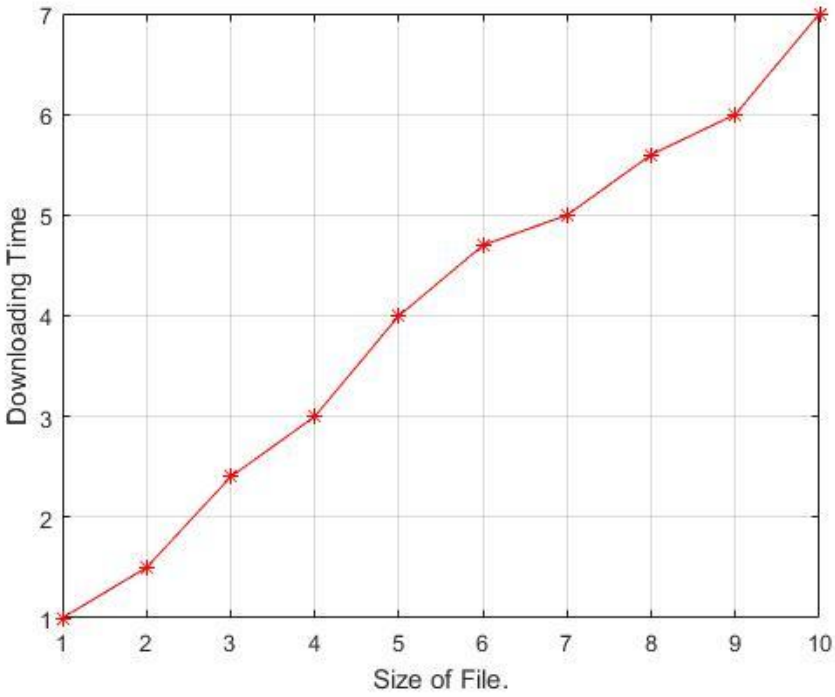

Fig: 4 Time Required for Download

VI. ADVANTAGES OF THE PROPOSED MODEL

Point for discussion	Identification Based Models	File Encryption Based Model	Secured channel using models	Proposed Model
Ways of ensuring security	Only identify the authorized person	Key and file both remain in one server. So, getting access on one server helps to get all information	Intruder can't access the data but uploaded file is not secured	Ensures security in data exchanging process. Only getting control over full system can leak information
Information leakage probability	Medium	Medium	Medium	Low
Complexity	Low	Medium	Low	Medium
Ensuring User Authentication	Main theme	If key is chosen by user, then slightly authenticate user	Probably not maintained	One-time password system is used for user authentication
Execution Time	Small	Medium	Small	Medium
Security Breaking Probability	Medium	Medium	Medium	Probably Low than others
Security Level	Medium	Medium	Medium	Higher than others model

VII. CONCLUSION

In this paper we proposed a security architecture for cloud computing system which is consist on AES file encryption system and Elliptic cryptosystem for secure communication. Onetime password for user authentication and SHA2 algorithm for hiding data. This model ensures security for entire cloud computing system. Here, execution time is not subsequently high because implementation of algorithm is done in different servers. In our proposed system, an intruder cannot easily get information and upload the files because he needs to take control over all the servers, which is quite difficult. The model, though it is developed in a cloud environment, individual server's operation has got priority here. So, decision taking is easy for each server, like authenticate user, give access to a file etc.

In future we want to work with ensuring secure communication system between users and system, user to user. We also want to work with encryption algorithms to find out more light and secure encryption system for secured file information preserving system.

REFRENCES

[1] Ijifr VE. Load Balancing And Security In Multicloud IaaS Using Distributed File System- A Review. International Journal of Informative & Futuristic Research; Volume 2 Issue 4 December 2014 International, ISSN (Online): 2347-1697;IJIFR/ V2/ E4/ 039 Page No. 1051-1055 Research.

[2] Kumar R, Pandey A. A Survey on Security Issues in Cloud Computing. IOSR J Comput Eng. 2016;3(3):506-517. doi:10.15680/IJIRSET.2016.0510073

[3] Vouk M a. Cloud computing — Issues, research and implementations. ITI 2008 - 30th Int Conf Inf Technol Interfaces. 2008:235-246. doi:10.1109/ITI.2008.4588381

[4] Hu Y, Wong J, Iszlai G, Litoiu M. Resource Provisioning for Cloud Computing. published 2009 in CASCON (Center for Advance Studies Conference) DOI:10.1145/1723028.1723041

[5] Ahead S. Cloud Computing : Silver Lining or Storm Ahead?.IA News Letter The Newsletter for Information Assurance Technology Professionals Volume 13 Number 2 • Spring 2010.

[6] Catteddu D, Hogben G. The European Network and Information Security Agency (ENISA) is an EU agency created to advance This work takes place in the context of ENISA ' s Emerging and Future Risk programme . C ONTACT DETAILS : This report has been edited by. Computing. 2009;72(1):2009-2013. doi:10.1007/978-3-642-16120-9_9

[7] Jamil D, Zaki H, Carlin S, Curran K. Cloud Computing Security. Int J Ambient Comput Intell. 2011;3(1):14-19. doi:10.4018/jaci.2011010102

[8] Kumar G, Chelikani A. Analysis of Security Issues in Cloud Based E-Learning. Secur Manag. 2011:1-74.

[9] Shan L. Journal Of Computers and math.pdf; Recent Advances in Intelligent Information Technology& Network Security; ISSN 1796-203XVolume 6, Number 10, October 2011.

[10] Sadeghi A, Schneider T, Winandy M, Horst G. Token-Based Cloud Computing. TRUST 2010;2: LNCS 6101, pp. 417–429; Springer-Verlag Berlin Heidelberg.

[11] Group TC. Solving the Data Security Dilemma with Self-Encrypting Drives. International Journal of Recent Research Aspects(IJRRA) ISSN 2349-7688 2010;May[12].

[12] Kokane M, Jain P, Sarangdhar P. Data Storage Security in Cloud Computing. Int J Adv Res Comput Commun Eng. 2013;2(3):1388-1393.

[13] Bugiel S, Stefan N, Sadeghi A, Schneider T. Twin clouds: An architecture for secure cloud computing,2011:1 11.http://www.zurich.ibm.com/~cca/csc2011/submissions/bugiel.pdf.

[14] Vaquero LM, Rodero-Merino L, Morán D. Locking the sky: A survey on IaaS cloud security. Comput (Vienna/New York). 2011;91(1):93 118. doi:10.1007/s00607-010-0140-x

[15] Thuy D, Nguyen TD, Gondree MA, et al. A Cloud-Oriented Cross-Domain Security Architecture A Cloud-Oriented Cross-Domain Security Architecture. 2010;(November):1701-1707.

[16] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou. Ensuring data storage security in Cloud Computing. 2009 17th Int Work Qual Serv. 2009:1-9. doi:10.1109/IWQoS.2009.5201385

[17] Kaufman LM. Data Security in the Cloud World of Cloud Computing. Ieee. 2009:61-64.

[18] Thuraisingham B, Khadilkar V, Gupta A, Kantarcioglu M, Khan L. Secure data storage and retrieval in the cloud. Proc 6th Int ICST Conf Collab Comput Networking, Appl Work. 2010. doi:10.4108/icst.collaboratecom.2010.15

[19] Hamlen K, Kantarcioglu M, Khan L, Thuraisingham B. Security Issues for Cloud Computing. Int J Inf Secur Priv. 2010;4(2):36-48. doi:10.4018/jisp.2010040103

[20] Abutaha M, Abutaha MS, Amro AA. Using AES , RSA , SHA1 for Securing Cloud. 2015;(April 2014).

[21] Bhardwaj A, Subrahmanyam GVB, Avasthi V, Sastry H. Security Algorithms for Cloud Computing Environment Security Algorithms for Cloud Computing. Procedia - Procedia Comput Sci. 2016;85(December 2015):535-542. doi:10.1016/j.procs.2016.05.215

[22] Arora R, Parashar A. Secure User Data in Cloud Computing Using Encryption Algorithms. International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-19262013.

[23] Salim E, Harba I. Secure Data Encryption Through a Combination of AES, RSA and HMAC. Engineering, Technology & Applied Science Research Vol. 7, No. 4, 2017, 1781-1785:1781-1785.

[24] Johnsson M. Mobile One Time Passwords and RC4 Encryption for Cloud Computing. 2011; Technical report, IDE1108 (March).

[25] Khan AA. Preventing Phishing Attacks using One Time Password and User Machine Identification. International Journal of Computer Applications (0975 – 8887) Volume 68– No.3, April 2013:7-11.

[26] Nadu T. Research Issues on Elliptic Curve Cryptography and Its applications. IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.6, June 2009:19-22.

[27] Verma SK, Ojha DB. A Discussion on Elliptic Curve Cryptography and Its Applications. IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012 ISSN (Online): 1694-0814:74-77.

[28] A.MEKMC, Phil M, Sc JM, Phil M, Ph D. Secure Login Using Encrypted One Time Password (OTP) and Mobile Based Login Methodology. Research Inventy: International Journal Of Engineering And Science Vol.2, Issue 10 (April 2013), Pp 14-17 Issn(e): 2278-4721.

[29] 6 Saini T. One Time Password Generator System. International Journal of Advanced Research in Computer Science and Software Engineering Research, Volume 4, Issue 6, June 2014 ISSN: 2277 128X

[30] Soni S, Singh SP. Secure and Efficient Integrity Algorithm based on Existing SHA Algorithms. International Journal of Computer Applications (0975 – 8887) Volume 113 – No. 11, March 2015:34-37.