Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 12, December 2019, pg.59 – 63

A Novel Approach for Cloud Data Security Enhancement through Cryptography and Biometric in the Government Cloud Environment

Pawitar Dulari[1]; Brijender Bhushan[2,*]
[1]Department of Physics, Government PG College Una (H.P.)-174303
[2]Department of Zoology, Pandit Sant Ram Government Degree College Baijnath (H.P.)-176125
E-mail: bantu.sls@gmail.com
*Corresponding author

Abstract: ***Cloud computing is next generation technology. It takes the technology, services, and applications that are akin to the raised mentioned on the Internet and swings them into a buffet utility. It is the distribution of computing as a service in lieu a product through which shared resources, software and information is provided to computers. Nowadays a single server handles the multiple requests from the user. Here the server has to process the one and the other request from the user simultaneously, so the processing time will the large. This may leads to damage of data and packets may be delayed and corrupted and also the Data Management and the Services are not reliable. Users start bothering about losing control of their individual data. Again the data processed on clouds are normally outsourced, leading to an amount of issues associated to liability, consisting of the handling of individually identifiable information. A useful TORDES is expected and implemented in view of this paper. The TORDES will explain us how to place the files efficiently to the containers in object storage. Besides, the files will join when client calls for it back. So some further algorithms are again used for partitioning and joining of files. So the goal is to attain good security for cloud storage system, over proposed algorithm by using legion containers of object storage in cloud. To handle these concern, the paper suggested an approach to stock the data over TORDES, to provide authentication and secure access control for data using Crypto-Biometric System (CBS) in cloud computing and to assure the data from unauthorized access.***

Keywords: Cloud Computing, Data Security, TORDES, Crypto-Biometric System.

I. INTRODUCTION

Cloud computing conveys enormously versatile registering resources as a services with Internet based advancements. Resources are shared among an incomprehensible number of customers taking into account a lower expense of IT proprietorship. At present, cloud computing is broadly examined in the technology world and industry. Virtualization, circulated registering innovation etc, cloud computing incorporates the processing, storage, organizing and other figuring resources, and afterward rents to clients. Such mode could decrease the expense of big business data development and quicken the information of big business. The Cloud storage is intended for virtualized PC environment. The cloud storage is actualized utilizing cloud computing that implies using the product and equipment resources of the cloud computing services supplier. Cloud computing is developing at a high speed in the IT business around the globe. While there are numerous points of interest of cloud computing, the undertakings are as yet holding up to utilize cloud computing, on account of the information security issue of cloud computing is not illuminated totally. Cloud storage gives a virtual space to store mass information. Be that as it may, the information proprietors have no power over their information. The cloud supplier has full control on the client's information. This makes the client's psyche to thing about the information security in the cloud. The data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information. To allay users' concerns, it is essential to provide an effective mechanism based on the notion of information accountability for users to monitor the usage of their data in the cloud. Our contribution to addressing these problems is a Privacy Manager, which helps the user manage the privacy of their data in the cloud. As a first line of defence, the privacy manager uses a feature called obfuscation, where this is possible. The idea is that instead of being present unencrypted in the cloud, the user's private data is sent to the cloud in an encrypted form, and the processing is done on the encrypted data. The result of the processing is de-obfuscated by the privacy manager to reveal the correct result. The obfuscation method uses a key which is chosen by the user and known by the privacy manager, but which is not communicated to the service provider. Thus the service provider is not able to de-obfuscate the user's data, and this data is not present on the service provider's machines, reducing (or even eliminating) the risks of theft of this data from the cloud and unauthorized uses of this data. Moreover, the obfuscated data is not personally identifiable information, and so the service provider is not subject to the legal restrictions that apply to the processing of the unobfuscated data. Where obfuscation is practical, the principle of data minimization gives a legal impetus to use it. However, it is not practical for all cloud applications to work with obfuscated data. For applications for which users have to upload some private data to the cloud, the privacy manager contains two additional features, called preferences and personae, which help the users to communicate to service providers their wishes for the use of this personal data, and thus assist the service providers to respect privacy laws requiring users' consent. The preferences feature allows users to set their preferences about the handling of personal data that is stored in an unobfuscated form in the cloud. It communicates these preferences to a corresponding policy enforcement mechanism within the cloud service. The preferences can be associated with data sent to the cloud, and preferably cryptographically bound to it (by encrypting both the policy and data under a key shared by the sender and receiver).For stickiness of the privacy policy to the data, public key enveloping techniques can be used. Alternatively, it is possible to use policy-based encryption of

credential blobs. Part of the preference specification could involve the purpose for which the personal data might be used within the cloud, and this could be checked within the cloud before access control were granted, using mechanisms specified. The personal feature allows the user to choose between multiple personae when interacting with cloud services. The user's choice of persona provides a simple interface to a possibly complex set of data use preferences communicated to the service provider via the preference feature, and may also determine which data items are to be obfuscated. A proposed efficient data placement algorithm is used. This will consider how to place the files efficiently to the containers in object storage. Besides, the files will merge when client needs it back. So some additional algorithms are also used for partitioning and merging of files. This paper extends the basic idea to store the data through TORDES algorithm, to provide authentication and secure access control for data using Crypto-Biometric System (CBS) in cloud computing and to Protect the data from unauthorized access.

II. LITERATURE SURVEY

This paper introduced brief analysis on data security in cloud environment. It is identified and presented as challenges in data security. There are still many actual problems that need to be solved and data are migrating to public or hybrid cloud.[1].The digital signature and Diffie Hellman key exchange blended with AES encryption algorithms to protect confidentiality of data stored in cloud. It takes more time to stored or accessing data in cloud [2].The hardware consumption is minimized. For this, implementation has been made using 32-bit block size & makes open to attacks [3]. The TORDES Algorithm and digital signature with encryption model is highly secured and light encryption system information has been processed [4]. Combined biometric Cryptography as crypto-biometric system was proposed to enhance the network security [5]. Enhancement of security of cloud and strong authentication has been explained in paper [6]. The key security considerations and challenges are currently faced in the cloud computing[7]. The various security algorithms, security issues and security attacks in cloud computing are discussed in paper [8]. The paper [9] deals with comparison of seven algorithms, five algorithms for symmetric algorithm and two for asymmetric algorithm for data security. Authors Compared various Security algorithms for data security in cloud computing. Based on the study of paper [10], TORDES algorithm was suggested as more secure and fast in speed of access wherein the TORDES algorithm was best but there is not practical results/examples. Implementation of TORDES algorithm for security over data provides benefits of less memory consumption and less computation time as compared to other algorithms which was discussed in paper [11]. The security of data is ensured by applying a method RSA algorithm [12]. Regarding the file size reflecting only in indexing process and not affecting the data protection gives strong protection. But it is not tested with the low and medium protection technique [13].

III. METHODOLOGY

The figure 1 deals with biometric authentication that creates DB based on the features Extracted from IRIS image for the New Client. This verifies DB and Provide Authentication with the Existing Client. This results in an efficient algorithm which is the best algorithms for IRIS recognition. And TORDES – cryptographic random key generation which proposed with a TORDES algorithm for more security and preventing attacks.

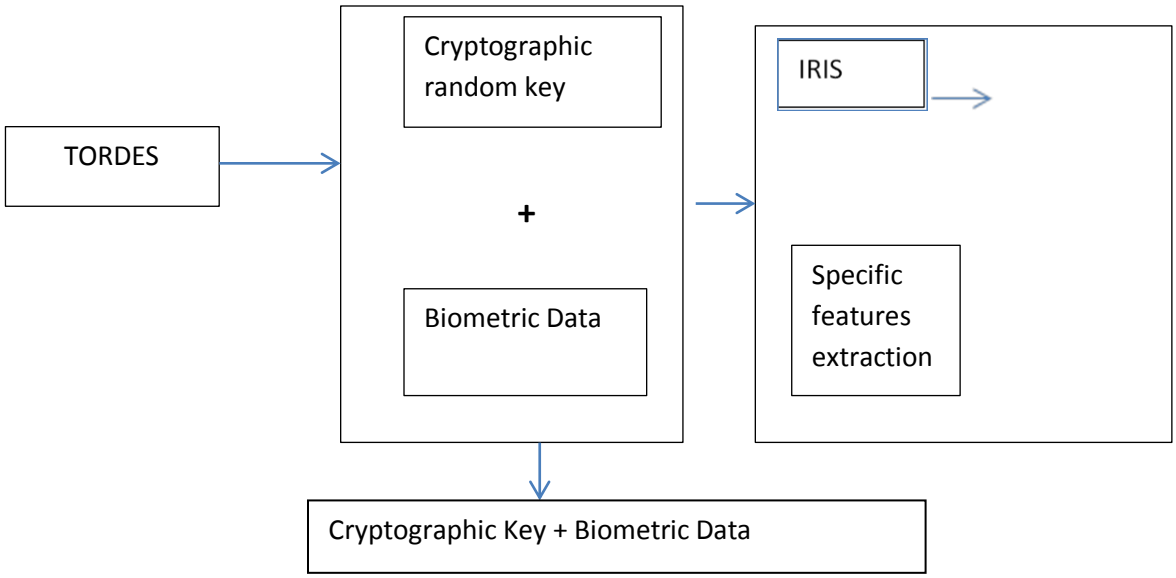

Fig.No.1. Proposed model

IV. TORDES

TORDES is a block cipher algorithm (Bhushan et al., 2012). It is a unique and independent approach which uses several computational steps along with string of randomized operators and delimiter selections by using some suitable mathematical logic with transformation and mirror image operation. It is specially designed to produce different cipher texts by applying same key on same plain text. It is one of the best performing partial symmetric key algorithms particularly for the text message in its class. It also safeguard against various attacks like Brute-force because it is not fully dependent on the key and code cannot be deciphered by applying all possible combinations of keys. The following information invariably used in TORDES for encryption techniques.

1) 32 bit key.
2) Code sequence string generated from a particular process (Multithread).
3) Transformation of string.
4) Mirror image of string.
5) Lookup Table
6) Randomized delimiter string This shows that the security of text data is not only depends upon key value. This really increases the security of text file.

V. CONCLUSION

The conclusion of the paper shows that the software and information has been provided to computers which are described as a service rather than a product. As a single server that handles the multiple requests from the user, the delay in data management of loss of data and packet management is reduced by applying the TORDES algorithm (biometric authentication) of the paper. The data storage on un-trusted cloud makes as a security issue. Data security in the cloud is guaranteed by the privacy of delicate information should be enforced on Cloud storage. Also reduces users botheration about losing control of their own data. This has fetched efficient and effective outcome by the proposed model. Finally, to store the data through data placement algorithm, to assure authentication and secure access control for data using Crypto-Biometric System (CBS) in cloud computing and to protect the data from unauthorized access has been made.

REFERENCES

[1] Meenakshi et.al., Data security analysis in cloud environment, International journal of innovations & advancement in computer science vol.2(1),pp.14-19,2014.
[2] Prashant rewagad and yogar , Use of digital signature with Diffie Hellman key Exchange and AES encryption algorithm to enhanced data security in cloud computing, International Journal of Scientific and Research Publications, vol.3(13),pp.437-439,June 2015.
[3] Prasanthi and Subba , Enhanced AES Algorithm, International Journal of Computer Applications in Engineering Sciences, vol 2 (2),pp.114-118,June 2012.
[4] Bhushan, A., 2012. "Transform Operator Random Generator Delimiter based Encryption Standard (TORDES)". CCIT2012, Iraq, , College of Computer, University of Anbar, Ramadi, Iraq 27th-28th March 2012.
[5] Subhas Barman, Samiran Chattopadhyay Debasis Samanta, An Approach to cryptographic key Exchange using Fingerprint, Springer-Verlag Berlin Heidelberg 2014.
[6] Abdullah A.Albahdal , Terrance E.Boult, Problems and promises of using the cloud and biometrics, 11th ICIT,2014.
[7] Kuyoro S.O, Lbikunle F, Awodele O, Cloud computing Security Issues and challenges, International Journal of Computer Science and Information Technology & Security, vol-3.2011.
[8] K.S.Suresh, K.V.Prasad, Security Issues and security algorithms in cloud computing, International Journal of Advanced Research in Computer Science and Software Engineering, vol-2,October, 2012.
[9] Bhushan, A., Bhartee, A., Dulari,, A Study of TORDES with other Symmetric Key Algorithms in Computer Science , 2.6, December, 2013: 270-274.
[10] A Study of TORDES with other Symmetric Key Algorithms Journal of Advanced Research in Computer Science and Software Engineering 3.3 pp.nos. 279-283, March, 2013.
[11] Abha, Mohit, and Mohit Bhansali, Enhancing cloud computing security using AES Algorithm, International Journal of Computer Applications pp.nos.67.9, 2013.
[12] Kalpana, Parsi, and Sudha Singaraju, Data security in cloud computing using RSA algorithm, International Journal of Research in Computer and Communication Technology 1.4, pp.nos.143-146, 2012.
[13] Sawdekar, Poonam, and Seema Shah, Implementation of Information Leakage Avoiding (ILA) Application in Cloud Computing , International Journal of Computer Applications pp.nos.97.13, July, 2014.
[14] IBM Corporation, IBM Bluemix [Online] Available https //www bluemix net/
[15] Tiancheng Li; Ninghui Li; Jian Zhang; Molloy, I.,Slicing: A New Approach for Privacy Preserving Data Publishing, Knowledge and Data Engineering, IEEE Transactions on, vol.24, no.3, pp.561-574,2012.
[16] Dulari, P., Bhushan, A., 2012. "*Crypto Analysis with A Symmetric Key Algorithm TORDES*", select in NCMIRA 2012, SMVD University Katra, 21 Dec-22 Dec 2012.
[17] Bhushan, A., Dulari, P., 2012 "*Component of Symmetric key Algorithm TORDES with its Functionality*", published in International Journal of Computational Engineering & Management, e-ISSN 2230-7893, Sep 5, 2012
[18] Bhushan, A. 2012. "Transform Operator Random Generator Based Encryption Standard". M.Tech. Dissertation. Mahamaya Technical University, Noida (U.P.)-India.
[19] Bhushan, A., 2012. "*TORDES: A New Approach To Symmetric Key Encryption*", Lambert Academic Publishing, 2012, ISBN 3659218413, 9783659218415.

