ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

Secure User Data In Cloud Computing By Using Encryption Algorithms

[1] S.R.Srividhya , [2] CH.Venkatesh, [3] Makapatti Siddharth
[1] Asst. Professor, Department Of CSE, BIHER
[2] [3] UG Student Department Of CSE, BIHER,Chennai-73, Tamil Nadu, India

Abstract: ***Cloud Computing is transforming information technology. As opinion and processes are migrating to the cloud, it is transforming not by yourself where computing is finished, but plus fundamentally, how it is finished. As increasingly more corporate and academic worlds invest in this technology, it will along with drastically fiddle subsequent to IT professional's functional atmosphere. Cloud Computing solves many problems of enjoyable sufficient computing, including handling peak omnipotent quantity, installing software updates, and, using excess computing cycles. However, the association technology has in addition to created tally challenges such as data security, data ownership and trans-code data storage. In this paper we have discussed nearly cloud computing security issues, mechanism, challenges that cloud relief provider slope during cloud engineering and presented the metaphoric testing of various security algorithms.***

Keywords: Secure, Cloud Computing, User Data, Encryption

I. INTRODUCTION

Cloud Computing is the completion to entrance a pool of computing resources owned and maintained by a third party via the Internet. It is not a supplementary technology but a way of delivering computing resources based in report to long existing technologies [1]-[5] such as server virtualization. The cloud is composed of hardware, storage, networks, interfaces, and facilities that present the means through which users can right of entry the infrastructures, computing proficiency, applications, and facilities a propos the order of demand which are independent of locations. Cloud computing usually involves the transfer, storage, and dealing out of information around the provider's infrastructure, which is not included in the customers control policy.

The concept Cloud Computing is joined adjacent those of Information as a Service (IaaS), [7,8,9] Platform as a Service (PaaS), Software as a Service (SaaS) all of which means facilitate oriented architecture [1]. Here comes the first gain of the Cloud Computing i.e. it reduces the cost of hardware that could have been used at fan decrease. As there is no showing off to build up data at adherent's mixture less because it is already at some new location. So otherwise of buying the amassed infrastructure required to manage the processes and save bulk of data which you are just renting the assets according to your requirements.

1) EXPERIMENTAL DETAILS

An investigative review presented in [6] is followed in this research do something to court injury out the comparison for rotate approaches connected which are absolutely connected to encryption techniques used for data confidentiality. The focus of this evaluation is to locate out the resolved for encryption failure during cloud storage process. Some researchers contribute their efforts in data accurateness as taking into account than ease as efficiency in [3]. In [8] evaluation process was adopted partially for comparing encryption techniques in cloud computing.

II. SYSTEM ARCHITECTURE

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

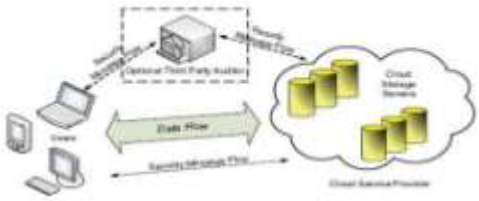

Fig 2.1. system architecture

Putting all together, our system is structured as follows:

We have a number of users who, back uploading to the Cloud,[10]-[15] split data into blocks (the data chunking technique that best fits your data), encrypt blocks gone convergent encryption and send to the server (or gateway) encrypted blocks together past their linked encrypted keys.

A server/gateway that additional encrypts blocks and keys afterward than a set of unique and unnamed keys. A metadata superintendent that updates the metadata (in order to rebuild the structure of each file) , stores encrypted block keys and performs[16]-[20] de duplication upon encrypted blocks. Only those blocks that are not already stored are actually stored.

A storage accrual to accrual single blocks, which can be seen as files/objects of little size. Since our system is unconditionally storage agnostic, we can accept the storage exaggeration once any storage system/provider. For instance, we might use a cloud storage provider such as Amazon S3, a distributed storage, a local file system, etc. The inverse process (download and decryption) is handy. It's important to narrowing out that thanks to our design, no single component has sufficient opinion to decrypt blocks or keys. Indeed, blocks[21,22] and keys are encrypted by users and the server/gateway. While this unbending idea might seem within attain, it's surprising to see how full of cartoon its and how dexterously it fits for various use cases.

A typical use suit might be the as soon as: the employees of a gigantic enterprise twinge to collect their data in the Cloud even though keeping data confidentiality and minimizing the amount of storage sky consumed. In this context, the server/gateway can be deployed upon the premises of the enterprise and the metadata superintendent can be deployed either locally or remotely (if we admiring to rely upon an encouragement provider for the de duplication and key government services).

III. ALGORITHM

3.1 AES ALGORITHM

The Advanced Encryption Standard, or AES, is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

3.2 FEATURES

Security: Competing algorithms were to be judged on their ability to resist attack, as compared to other submitted ciphers, though security strength was to be considered the most important factor in the competition.

Cost: Intended to be released under a global, nonexclusive and royalty-free basis, the candidate algorithms were to be evaluated on computational and memory efficiency.

Implementation: Algorithm and implementation characteristics to be evaluated included the flexibility of the algorithm; suitability of the algorithm to be implemented in hardware or software; and overall, relative simplicity of implementation.

3.3 CHOOSING AES ALGORITHM

Fifteen competing symmetric key algorithm designs were subjected to preliminary analysis by the world cryptographic community, including the National Security Agency (NSA). In August 1999, NIST selected five algorithms for more extensive analysis. These were:

- MARS, submitted by a large team from IBM Research
- RC6, submitted by RSA Security
- Rijndael, submitted by two Belgian cryptographers, Joan Daemen and Vincent Rijmen
- Serpent, submitted by Ross Anderson, Eli Biham and Lars Knudsen
- Twofish, submitted by a large team of researchers from Counterpane Internet Security, including noted cryptographer Bruce Schneier

3.4 METHODS

3.4.1 HOW AES ENCRYPTION WORKS

AES comprises three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. The Rijndael cipher was designed to accept additional block sizes and key lengths, but for AES, those functions were not adopted.

3.4.2 AES encryption block cipher

Symmetric (also known as secret-key) ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know -- and use -- the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of ciphertext.

The AES encryption algorithm defines a number of transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array; after which the cipher transformations are repeated over a number of encryption rounds. The number of rounds is determined by the key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

The first transformation in the AES encryption cipher is substitution of data using a substitution table; the second transformation shifts data rows, the third mixes columns. The last transformation is a simple exclusive or (XOR) operation performed on each column using a different part of the encryption key -- longer keys need more rounds to complete.

IV. CONCLUSION

Cloud computing is usefully one of today's most enticing technology areas due, at least in allocation, to its cost efficiency and malleability. The clouds have alternating architecture based more or less the facilities they present. The data is stored in this area to centralized location called data centres having a large size of data storage. The data as dexterously as admin is somewhere concerning servers. So, the clients have to trust the provider upon the availability as proficiently as data security. Before moving data into the public cloud, issues of security standards and compatibility must be addressed. A trusted monitor installed at the cloud server that can monitor or audit the operations of the cloud server. In minimizing potential security trust issues as capably as adhering to governance issues facing Cloud computing, a prerequisite rule undertaking is to ensure that a definite Cloud computing Service Level Agreement (SLA) is enlarge place and maintained once dealing in addition to than outsourced cloud further providers and specialized cloud vendors. Cloud computing promises to regulate the economics of the data centre, but since indulgent and regulated data liven up opinion into the public cloud, issues of security standards and compatibility must be addressed including sound authentication, delegated attributed approval, and key turn for encrypted data, data loss protections, and regulatory reporting.

REFERENCES

1. Kavitha, R. Shelgin, S.,, Sandeep, S. "A study on vulnerability detection of attacks in web security",2017,International Journal of Pure and Applied Mathematics,Volume 116,10 Special Issue, Page No: 9-12
2. Kavitha, R., Priya, N., Anuradha, C., "Li-Fi science transmission of knowledge by way of light",2017, International Journal of Pure and Applied Mathematics, Volume 116,9 Special Issue, Page No:285-290
3. Kavitha, R..,Priya, N., Anuradha, C., "A novel approach of hybrid cloud",2017, International Journal of Pure and Applied Mathematics, Volume 116, 9 Special Issue, Page No:299-304
4. Kavitha, G., Kavitha, R., Koushik Subramaniam, Y. "Operating scheme and its shield in mobilephone by utilizing android",2017,International Journal of Pure and Applied Mathematics,Volume 116, 9 Special Issue, Page No:129-133
5. Kavitha, R., Kavitha, G."Deconstructing evolutionary programming using ghat",2017, International Journal of Pure and Applied Mathematics,Volume 116,10 Special Issue, Page No:213-216
6. Kavitha, R., Kavitha, G., Thakur, K.A. "Helmet mounted heads-up display a rider assistance smart helmet for everyone",2017,International Journal of Pure and Applied Mathematics, Volume 116,8 Special Issue, Page No:411-413
7. Priya, N., Pothumani, S., Kavitha, R,"Merging of e-commerce and e-market-a novel approach",2017,International Journal of Pure and Applied Mathematics,Volume 116,
9 Special Issue ,Page No:313-316
8. Priya, N., Anuradha, C., Kavitha, R" Analysis of various data mining clustering algorithms",2017,International Journal of Pure and Applied Mathematics,Volume 116, 9 Special Issue,Page No:279-281

9. Kavitha, S., Kavitha, R.”DDOS attack and defenses”,2017,International Journal of Pure and Applied Mathematics,Volume 116,9 Special Issue,Page No: 57-61
10. Kavitha, R., Kavitha, G.,”Decoupling byzantine fault tolerance from multi-processors in I/O automata”,2017,International Journal of Pure and Applied Mathematics,Volume 116,10 Special Issue,Page No:225-228
11. Kavitha, R., Kavitha, G.”A development of IPV4 with skilty approach”,2017, International Journal of Pure and Applied Mathematics,Volume 116,10 Special Issue, Page No:219-222
12. Shelgin, S., Kavitha, R.”A cram on bluejacking by OBEX (Object exchange)”, Volume 2017, International Journal of Pure and Applied Mathematics,Volume 116,9 Special Issue, Page No:441-445
13. Shelgin, S., Kavitha, R., Sudha, K.L.”Identifying credit card fraud using biometric fingerprint techniques”,2017,International Journal of Pure and Applied Mathematics,Volume 116,9 Special Issue, Page No: 447-451
14.Kavitha, G., Kavitha, R., Jennifer, S.“Effectual exploit of digital irrigate tecniques to afford cloud safety marking”,2017,International Journal of Pure and Applied Mathematics, Volume 116,8 Special Issue,Page No:185-189
15. Kavitha, R., Kavitha, G., Ramya, B.”Inpatient monitoring for healthcare data using wireless sensor network”,2017,International Journal of Pure and Applied Mathematics, Volume 116,9 Special Issue, Page No:345-350
16. Kavitha, R. “A methodology for improving read-write technologies for dhts”,2017, International Journal of Pure and Applied Mathematics, Volume 116,8 Special Issue, Page No:93-97
17. Priya, N., Pothumani, S., Kavitha, R.”Analysis of data mining using social network”, 2017,International Journal of Pure and Applied Mathematics,Volume 116, 9 Special Issue, Page No: 307-310
18. Shelgin, S., Kavitha, R.”A study on web application security state”,2017,International Journal of Pure and Applied Mathematics, Volume 116,9 Special Issue, Page No:75-78
19. Priya, N., Anuradha, C., Kavitha, R.”Analysing storage and processing in enhanced cloud computing with hadoop “, 2017, International Journal of Pure and Applied Mathematics,Volume 116,9 Special Issue,Page No:293-296
20. Kavitha, G., Kavitha, R.,Indhu.G, “Big Data, Cloud, Web of Thing in Healthcare Monitoring Scheme”, 2017, International Journal of Pure and Applied Mathematics, Volume 116,8 Special Issue, Page 177-182
21. Kavitha, R., Kavitha, G., “Fuzzy, probabilistic algorithms for online clustering algorithms”,2017, International Journal of Pure and Applied Mathematics,Volume 116,10 Special Issue, Page No:207-211
22. Shelgin, S., Kavitha, R., Balasubhakar,”A comparitive study on 5g mobile wireless technology”2017,International Journal of Pure and Applied Mathematics, Volume 116, 9 Special Issue,Page No:81-85