International Journal of Engineering & Technology, *7 (1) (2018) 152-156*

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i1.8340
Research paper

Enhancing security for end users in cloud computing environment using hybrid encryption technique

Nadesh R.K[1*], Srinivasa Perumal R[1], Shynu P.G[1] and Gaurav Sharma[1]

[1]*School of Information Technology and Engineering, VIT University*
[*]*Corresponding author E-mail: rknadesh@gmail.com*

Abstract

In the era of cloud, anything and everything as a service facilitates number of remote user connected from anywhere, anytime and any form of access to the storage services. Today, Cloud storage has bceome an essential aspect of cloud computing, stores information and support any kind of applications. Applications like Internet of Things, Big Data analytics, Data warehousing, Databases, Backups and archive applications all rely on some form or the other on cloud storage architecture. Users may have a different variants of smart devices such as tablet, PCs, notebook and smart phones. Cloud storage provides an interlink between these smart devices. Enterprises prefer to use cloud storage because they provide cost-friendly and flexible alternatives on locally implemented hardware. However, business process in the cloud needs secured transaction, confidential files are sometimes exposed to risk of leakage, as cloud- stored data resides outside of the local infrastructure, thus vulnerable to security risks. Cloud storage providers provides enough security at their end, but there is no system that provides client level security while using public clouds. The proposed system will provide client level security using hybrid encryption techniques. Using AES (Advance Encryption Standard) in CBC Mode (Cipher Block Chaining) and HMAC-SHA-1 (Hash-based Message Authentication Code) with light weight methods enhances the strong encryption at client level security. Fusion of these algorithms adds extra layers of security to the cloud storage data. The proposed method enhances the security measures for any client users, using storage as a service offered by serval cloud service providers

Keywords: *Authentication; Cipher Block Chaining; Cloud Security; Cloud Storage; Encryption.*

1. Introduction

Computing paradigm shift has changed the entire world where everything without exception as an administration encourages the remote client associated from anyplace whenever and access to the capacity administrations and access to the storage services. Larges number of cloud service providers facilitates with Storage as a Service and applications like Internet of Things, Big Data analytics,Data marting, Database as a Service, backups and archive applications all rely on some form or the other on cloud storage architecture. Cloud Storage are basically more reliable, secure and scalable then traditional local storage systems. In 2018, each user is expected to store at least 3.3 MB of their information in the cloud by the rising number of users for the commercial leaders in personal cloud storage like Dropbox and Google Drive. With expansion of cloud storage in smart devices like mobile, watches, health care and IOT devices, the amount of data collected is in petabytes daily and needs to be secured by using modern techniques.

Recent Studies of ”Cloud Security Alliance (CSA) and Georgia Technology Information Security Centre (GTISC)” shows how insecure API (Application Package Interfaces) poses data lose, data leakage threats and virus programs as outsiders can get access to unauthorized data. Use of cloud storage service would be needed to differentiate between cloud service providers. On an average 15.8% data on a cloud contain sensitive data, where 7.6% in file sharing services, 2.3% payment data and 1.6% protected health information and 4.3% personally identifiable information. Managing data on cloud is complicated and though according to the data of SANS institute 33% due to lack of visibility, 40% due to unauthorized access, 40% due to sensitive data and 33% due to cloud breaches. Cloud security poses more threats during data migration and during storage of unknown data. The cloud storage involves communication between client and cloud service provider. As intermediate communication involves protocol and are more prone to data security breach on both the sides, Thus this proposed method is to improve the end user level security to protect data on cloud.

Cloud storage security provider provides remote storage facility to the user but still exists the lack of trust between the client and the service provider.Even though they execute service level agreement ensuring the end-to-end security but still the client side is not updated with latest security measures. Service providers provides security with latest encryption techniques but, still it is difficult to trust them so it is very important to provide client side security that would allow only to that specific set of user to access data on cloud. Even if cloud services are compromised, data will not be accessed by unauthorized user. The proposed method ensures one layer security in addition to the security services provided by the cloud storage provider.

1.1. Challenges

As more and more application demands for higher information security at greater measuring from service provider to boost deference while appending more efficiency and use to become more spread. Encryption algorithms are additional price for service provider for cloud storage because of the computation power required for encryption of data before transferring to the remote storage provider.The methodology used for choosing cloud development storage, identifying the security needs for the client and cloud storage deployment is through the service providers. Like, an advertising squad using cloud computing memory for media and videos may only require encoding for their story credential. However, data should be kept securely in the different environment. Encryption must certainly be stored separately from the secured information to make certain data security. Key storing also should be kept separately from the following process of encryption of data. Key management id the recitation include periodically controlling keys, particularly if keys lifetime expired as used in the resource. Some companies generates their key automatically, but that could give unnecessary complexity in a few cases. The best practice for key management is to get the multi-factor authentication in the captain and encryption keys.

2. Literature Review

Large number of algorithms and methods are in the literature and gives a feel that Cloud storage security is regular research topic among the researchers.Hybrid encryption algorithm using symmetric encryption with embedding low typical codec[1].Data become random code in nature when it is out, the only way from which the information owner can recover the same. As cloud system storage more prone to information leakage at inner department thus the authors suggested to use checksum + block size to separate data from user personnel information. This not only minimize retention of information at the same time it assures data security by separating some key information.The whole work flow is comprises of two parts. They are storing stage and data exporting stage, Checksum 1 and the Timestamp would be kept in client environment of system. After that 2nd checksum is calculated and added to block size. Next, the random vector is added thus Random code with Checksum 2 and Block size is transmitted to transmission module. Next, session id is added to send uploading request to server. Server gives new storage space using storage controller. For retrieval data is decoded first and tested for "Checksum 1 and Timestamp. If it matches then further decryption takes place using private key[2].

Cloud storage confidentiality protection system with cloud encryption and obfuscation technique.Obfuscation technique to improve the data confidentiality in cloud system storage. They have shown that encryption and obfuscation technique can be done at client ends. They proposed database outsourcing model which will help user to utilize data efficiently as a centralize storage. Monitoring DBMS is hard as it is distributed among different hardwares. Thus, security becomes big concern in many virtual machines as we can access database without anyone noticing or setting off any alert[3].Malicious person can use situation on his hand and harm integral database system at risk. All the data must be encrypted or obfuscated before it is sent to the cloud database.For the client, it is giving permission by giving the required information decryption /decipher keys[4].

Security model for computing purpose uses different servers and every servers performs same computation in the network[5].To get integrity of information server will compute SHA-1" and finally server encrypts the data using AES to maintain confidentiality of data.Finally data is encrypted using AES to ensure confidentiality.

To protect data on the cloud using meta-data [6,7] the proposed technique provides generation of cipher using Meta data. It depends on number of attributes in meta-data and algorithm used. There are two main feature: Generated key cant be settled without association of user and Meta data storage server and Key generated using fiesta network hold good for the avalanche effect. It takes time to generate cipher key.

With this newspaper, most people provided a blueprint regarding encrypted shield regarding look-alike employing AES plus vision cryptanalysis[8]. The samara has been bought from the whole picture characteristics plus the AES-256 protocol was utilized to be able to create the essential beneficial for your graphic encrypted shield in accordance with the removed key. The protocol is really a symmetric obstruct cipher in which burn essential dimensions regarding 128, 192 plus 256 chunks, together with information managed inside 128-bit clog[9]. The particular pixel be aware importance from the photographs to generally be protected have been protected employing n-share vision cryptographic technique. The particular encrypted shield method encountered virtually no departure regarding pixel ideals through the entire process. The 128 little headstone will then be widened several 44 blog posts regarding 32 chunks Guide ; 4 different terms program like a leaflet essential for each around; essential agenda makes use of your S-box. The process is made of 3 layers? Straight line Diffusion, Non-linear Diffusion .The 128 little essential will then be widened several 44 blog posts regarding 32 chunks terms; 4 different terms be an around essential for any around; essential agenda would depend about the S-box. AES just serps obstruct very little assist every mixture of information plus essential sizes regarding 128, 192, plus 256[10] amounts. Nevertheless, AES basically enables the 128 little information time-span which can be split directly into a number of standard business mind block Each mix is produced by AES and make use of various circuits regarding predetermined expeditions to achieve ideal productivity which in turn can help determine it has the protection degree that is certainly tested inside phrase regarding dispersion (strict influx requirements (Sac)) plus bafflement for this reason the number of circuits tend to be picked inside a your protocol provides the Theca value. The essential style plus muscle of the encryption protocol this sort of regarding instance AES will be dependent about diffusion plus mind confusion. This involved use of Innovative File encryption protocol plus vision cryptography inside getting forensic biometric images.

The proposed arrangement suggests a different method of the way that the files are stored from the swarm by employing the existing encryption method and swarm computing system[11]. Most drug user are certainly not comfortable by knowing that their extremely private or confidential files could be accessed for assorted intent with the cloud Waiter provider. This may be for maintenance purposes, certificate thread claims or simply regular file backup physical processes. Normally, these grounds are complete valid in an effort to protect the cloud Waiter status and performance. However, users are often unwilling to upload their confidential files into cloud servers[12]. This proposed system aims to fill this breakthrough providing a high level tier of file protection. RSA is known to be the best publicly available encryption method. This algorithm harmonizes with both private key and public key. The only method of decrypting the files which have been encrypted with the population key is to use the non-public key. Users file might be encrypted just before the upload process towards the cloud Server. Exactly the encrypted file might be uploaded towards the Server. This proposed system intention to fill this gap by giving a professional amount of single file cabinet protection. RSA is known to be the best popularly available encryption method acting. This algorithm works with both private key and public key. To get of decrypting the files which have been encrypted with the public key is with the individual key[13,14]. Exploiter file might be encrypted just before the upload operation on the cloud Waiter. The encrypted file might be uploaded on the host.

Security model that contain three components: cloud controller, user and connected nodes. Delay measurement was performed on the basis of the request and response time during file upload. System they proposed is built on online file processing system consist of web application[15]. They used 128 bit AES encryption, where encryption consists of 10 rounds for 128-bit keys. The files are split into different chunks which depends on file size. Then particular blocks are encrypted separately and then after block wise encryption each blocks are uploaded to cloud at different locations with different id and block id. If someone like cloud provider, try to reach written documents completely from the server, they will not get whole data, because it stored at different locations as well as are in encrypted form[16]. Hence the individual who knows secret key can retrieve data back. Online editing is allowed in the proposed system, data can be changed without downloading the contain. Quality of service is maintained to reduce delay in the uploading[17]. The delay are vastly different in line with the size of web data being processed. On top of that, types of factors which affect delay inside the system: network speed is important but one essential aspect during actual time execution. 128 bit AES cryptographic encryption is used in these to provide authenticity, confidentiality, and access control. Then performance of proposed approach was analysed based upon delay[18], there's drastic surge in delay with surge in file size. User is authenticated using password verification.

K.Sekar and M.Padmavathamma et al proposed study of encryption in big data in cloud environment[19]. The key security issues of big data are near authentication level, data level, network level and generic level issues. Of these levels, we have decided you're the results level issue. In big data, statistics is quite vital component. Data hosted on social media sites is very necessary for an enterprise which is often within the public use or private zone. Data Confidentiality, Security, integrity and availability is actually a major challenge as of this degree[20]. It converts data into secret message using encoding algorithms. There are lots of algorithms like AES, RSA, and DES. These algorithms use private secrets to encrypt data and decrypt data. Encryption is conducted for the data sent from reservoir and decryption is conducted before the data is received. For encryption and decryption process, two case of algorithms are widely-used i.e., symmetric and asymmetric algorithms. Data Encryption Standard algorithm uses the aught Francis Scott Key called feistily block secret code. The function linked to accepting the plain text and key arrangement determines the kind of cipher. It uses "64-bit block cipher" for encoding and decipherment which is therefore known as Symmetric. Encrypting and decrypting symmetric key details are relatively simple to do. Many of the solid state drives use symmetric key encryption for internal reposting of data. This algorithmic program performs a lot better than unencrypted traditional hard drives.

Dta storage techniques for efficient and intelligent storage using data replication. Several new techniques are adapted to optimize the present generic architectures for developing softwares are as explained by the authors [21].

3. Proposed Method

The objective is to encrypt data at end user level so that it can be stored in cloud in protected environment and decrypt whenever required and a mechanism to do that using AES Algorithm in CBC mode and HMAC-SHA.

As the AES allows variable key lengths, the Key Length attribute have to be specified in both a Phase 1 exchange and a Phase 2 exchange.

3.1. AES-CBC Algorithm

1. AddingRoundKey(statein, w, param1, param2): this takes the $4 \times Nbi \times (Nri + 1)$ bytes of key P, w, and does an XOR of successive portions of the expanded key with the changing state array.
2. SubtituteBytes (statein): this takes each byte of the state and independently looks it security table to substitute a different byte for it.
3. ShiftRow (statein): this simply moves around the rows of the state array.
4. MixCols (statein): this does a much more complicated mix of the columns of the state array.

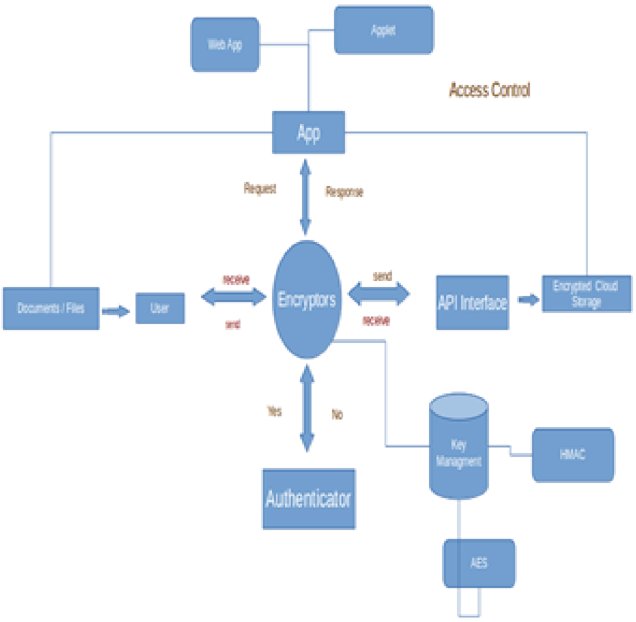

Figure 1: Architecture of the Proposed Method

AES-CBC Algorithm

```
AESCipher(byteof[] in, byteof[] out, byteof[] w)  Byte of [][]
  state = byteof[4][Nb];
statein = in;
AddingRoundKey(statein, w, 0, Nbi - 1);
for (roundin = 1; round ¡ Nri; round++) do
    SubtituteBytes(statein);
    statein;
    MixCols(statein);
    AddingRoundKey(statein, w,round*Nbi, (round+1)*Nbi -
      1);
end
SubBytes(statein);
ShiftRows(statein);
AddingRoundKey(statein, w, Nri*Nbi, (Nri+1)*Nbi - 1);
outof = statein;
```

Algorithm 1: AES-CBC Algorithm

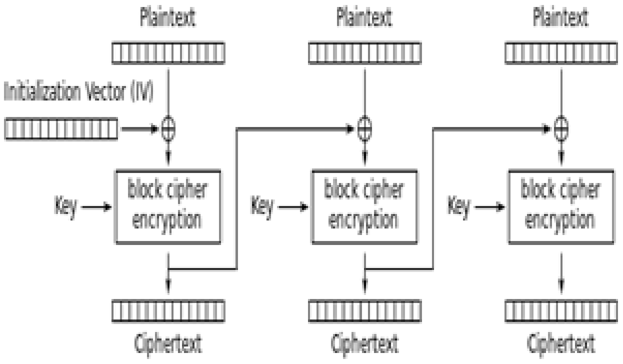

Figure 2: Cipher Block Chaining Encryption

3.2. HMAC with SHA256

Hash-based message authentication code (HMAC) provides client and cloud storage server each with private key which is only known to that server and that specific client.

$$HMAC(key, msg) = H((K0 \oplus OP)H((K0 \oplus IP)||msg) \qquad (1)$$

where || denotes Concatenation, H denotes Hash function, OP denotes Outer Padding and IP denotes Inner Padding

```
Algorithm HMAC (keyP, msg)
if (len(keyP) < blocksizeof) then
    // KeyP = hash (key) // keysP longer than blocksizeof are sliced
else
    if (len (keyP) < blocksizeof) then
        //blocksize are zero-padded
        KeyP = key ? [0x00 × (blocksizeof - len (keyp))]
        // Where * is repetition.
    end
end
o_ key_ pad_ i = [0 × 5c × blocksizeof] ⊕ keyp;
i_ key_ pad_ i = [0 × 36 × blocksizeof] ⊕ keyp;
Return hash(o_ key_ pad_ i, hash (i_ key_ pad_ i))
```

Algorithm 2: Hash-based message authentication code

Table 1: Standards in HMAC SHA

Algorithm ID	Block Size	Output Length	Trunc Length	Key Length	Algorithm Type
HMAC-SHA-256-128	512	256	128	256	Auth/Integ
HMAC-SHA-384-192	1024	384	192	384	Auth/Integ
HMAC-SHA-512-256	1024	512	256	512	Auth/Integ
PRF-HMAC-SHA-256	512	256	None	Var	PRF
PRF-HMAC-SHA-384	1024	384	None	Var	PRF
PRF-HMAC-SHA-512	1024	512	None	Var	PRF

For better understanding of proposed system different types of strings are passed to encrypt or and cipher text is obtained .Thus following Transaction table is used to show different strings and their encrypted form:

Table 2: Transaction Table

Tid	Plain Text	Cipher
1	$helloWorld	$MNJGWamX+jNw/Y8zL96HVw==
2	cloud	$F94qdBmmnZlfqMyqZXq4lQ==
3	545	$jOCWk6HQMoSp5H6JJoqZ0g==
4	$MyWorld545	$J0fBxnkP245lf5MqFOCj1g==

These Encryptions can also be used to encrypt audio, videos, documents etc. and store it on cloud storage. Using Public cloud storage API's like Drop box we have uploaded different type of data and retrieved back successfully using private key generated using HMAC.

3.3. Results and Discussion

Retrieval process involves downloading data and decrypting back to its original content using HMAC private key, whole process divided into two parts: retrieve and decipher. In retrieval phase with the help of public cloud API, download data, using shell script. In the decipher process, a private key is used to extract data and then using AES CBC Decryption Algorithm into an original shelf. To maintain uniqueness of message initial vector is being used. In CBC Mode each block is XORed with last-iterated block before actually encrypting data. Thus, for the decryption process each cipher text had to be XORed again with the plain text of the next block to get the original message back.

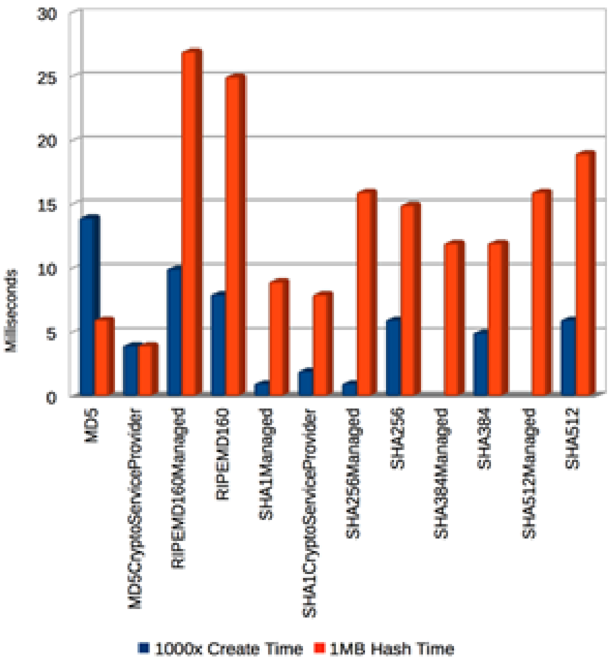

Figure 3: Performance of Hash Algorithm

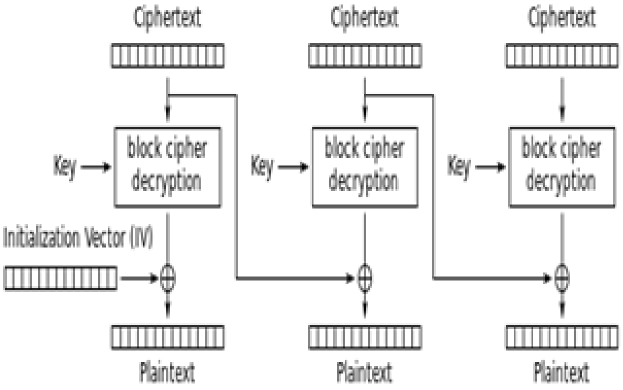

Figure 4: Cipher Block Chaining (CBC) Decryption

Table 3: AES Comparison

Algorithm	MiB/Second	Cycles Per Byte	Microseconds to Setup Key & IV	Cycles to Setup Key & IV
AES/GCM(2K tables)	102	17.2	2.946	5391
AES/GCM(64K tables)	108	16.1	11.556	21130
AES/CCM	61	28.6	0.888	1625
AES/EAX	61	28.8	1.757	3216
HMAC(SHA-1)	147	11.9	0.509	932
AES/CTR(128 Bit Key)	139	12.6	0.698	1277
AES/CTR(192 Bit Key)	113	15.4	0.707	1293
AES/CTR(256 Bit Key)	96	18.2	0.756	1383
AES/CBC(128 Bit Key)	109	16.0	0.569	1041
AES/CBC(192 Bit Key)	92	18.9	0.572	1046
AES/CBC(256 Bit Key)	80	21.7	0.619	1133
AES/OFB(128 Bit Key)	103	16.9	0.702	1285
AES/CFB(128 Bit Key)	108	16.1	0.926	1695
AES/ECB(128 Bit Key)	109	16.0	0.253	462

4. Conclusion

Data storage is the latest trend in ”Cloud computing. However, data security, reliability, utilizer’s solitude and also other difficulties within this professional organization could be critical elements in the lot of different Applications. As knowing about symmetric encryption, we should employee appropriate safety techniques. The technique which ought to guard the users secret key can’t be affected and can’t be violated through a ”virus or Trojan. The statistical analysis of cloud storage on unreliable data on cloud makes records safety as a big issue. Cloud safety inside the storage is approved by the confidentiality of sensitive statistics need to be forcing cloud system storage service companies. Thus Hybrid Encryption proposed in this paper can be used to give client level security” and provide reliability to cloud storage. Client level security ensure more trust of the user on cloud storage and ensures extra level of security for Cloud service providers. This is initial attempt to give end user protection, many different hybrid encryptions can be used for cloud storage protection.

References

[1] Maurich Ingo, Heberle Lukas, Güneysu Tim, ”IND-CCA Secure Hybrid Encryption from QC-MDPC Niederreiter”, *7th International Workshop on Post-Quantum Cryptography*, Vol.9606, (2016), pp.1–17.

[2] Usman Muhammad, Ahmed Irfan, Aslam M Imran , Khan Shujaat , Shah Usman Ali, ”SIT: A Lightweight Encryption Algorithm for Secure Internet of Things”, *arXiv preprint arXiv:1704.08688*, (2017).

[3] MDawahdeh Ziad E , Yaakob Shahrul N ,bin Othman, Rozmie Razif, ”A New Image Encryption Technique Combining Elliptic Curve Cryptosystem with Hill Cipher”, *Journal of King Saud University-Computer and Information Sciences*, (2017).

[4] Maurich Ingo, Heberle Lukas, Güneysu Tim, ”Efficient cloud storage confidentiality to ensure data security”, *International Conference on Computer Communication and Informatics*, (2014), pp.1–5.

[5] Zhao Gansen, Rong Chunming, Li Jin, Zhang Feng, Tang, Yong, ”Trusted data sharing over untrusted cloud storage providers”, *International Conference on Cloud Computing Technology and Science*, (2010), pp.97–103.

[6] Chen Deyan, Zhao Hong, ”Data security and privacy protection issues in cloud computing”, *International Conference on Computer Science and Electronics Engineering*, (2012), pp.647–651.

[7] Stanek Jan, Sorniotti Alessandro, Androulaki Elli, Kencl, Lukas, ”A secure data deduplication scheme for cloud storage”, *International Conference on Financial Cryptography and Data Security*, (2014), pp.99–118.

[8] Slamanig Daniel, Hanser Christian, ”On cloud storage and the cloud of clouds approach”, *International Conference on Internet Technology And Secured Transactions*, (2012), pp.649–655.

[9] Fathy Ahmed, Tarrad Ibrahim F, Hamed Hesham FA, Awad Ali Ismail, ”Advanced Encryption Standard Algorithm: Issues and Implementation Aspects”, *AMLTA*, (2012), pp.516–523.

[10] Al-Shawabkeh Mahmoud, Saudi Madihah Mohd, Alwi Najwa Hayaati Mohd, ”Computer security self-efficacy effect: An extention of Technology-to-Performance chain model”, *Control and System Graduate Research Colloquium*, (2012), pp.64–69.

[11] Karuppusamy Sasikumar , Muthaiyan Madiajagan, ”An Efficient Placement Algorithm for Data Replication and To Improve System Availability in Cloud Environment”, *International Journal of Intelligent Engineering and Systems*, Vol.9, No.4,(2016), pp.88–97.

[12] Jing Zhang , Jinsu Wang , Zhuangfeng Zheng , Chongan Zhao, ”Cloud storage encryption security analysis”, *International Conference on Cloud Computing and Big Data Analysis*, (2016), pp.62–65.

[13] Yahya Fara, Walters Robert J , Wills Gary B, ”Goal-based security components for cloud storage security framework: a preliminary study”, *International Conference On Cyber Security And Protection Of Digital Services*, (2016), pp.1–5.

[14] Nadesh RK, Jagadeesh Meduri , Aramudhan M, ”A Quantitative Study on the Performance of Cloud Data Centre: Dynamic Maintenance Schedules with Effective Resource Provisioning Schema”, *Indian Journal of Science and Technology*, Vol.8, No.23,(2015).

[15] Black John, Halevi Shai, Krawczyk Hugo , Krovetz Ted , Rogaway Phillip, ”UMAC: Fast and secure message authentication”, *Annual International Cryptology Conference*, (1999), pp.216–233.

[16] Patil Amit, Marimuthu K , Niranchana R, ”Comparative study of cloud platforms to develop a Chatbot”, *International Journal of Engineering & Technology*, Vol.6, No.3, (2017), pp. 57–61.

[17] Bellare Mihir, Kilian Joe, Rogaway Phillip, ”The security of the cipher block chaining message authentication code”, *Journal of Computer and System Sciences*, Vol.61, No.3, (2000), pp. 362–399.

[18] Black John, Rogaway Phillip, ”A block-cipher mode of operation for parallelizable message authentication”, *Advances in CryptologyEUROCRYPT*, (2002), pp. 384–397.

[19] Sekar K , Padmavathamma M, ”Comparative study of encryption algorithm over big data in cloud systems”, *International Conference on Computing for Sustainable Global Development*, (2016), pp. 1571–1574.

[20] Dhingra Mridula, Gupta Neha, ”Comparative analysis of fault tolerance models and their challenges in cloud computing”, *International Journal of Engineering & Technology*, Vol.6, No.2, (2017), pp. 36–40.

[21] Li Jin , Li Yan Kit , Chen Xiaofeng , Lee Patrick PC , Lou Wenjing, ”Comparative analysis of fault tolerance models and their challenges in cloud computing”, *IEEE Transactions on Parallel and Distributed Systems*, Vol.26, No.5, (2015), pp. 1206–1216.