International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 12, December-2014

A Security Service Algorithm to Ensure the Confidentiality of Data in Cloud Storage

Dr. L. Arockiam,
Associate Professor, Dept. of Computer Science,
St. Joseph's College (Autonomous)
Tiruchirappalli, Tamil Nadu, India.

S. Monikandan
Research Scholar,
ManonmaniamSundaranar University,
Tirunelveli, Tamil Nadu, India.

***Abstract*—Cloud computing dominates the IT industry's by its computing services. The main service provided by the cloud is data storage. Cloud has more sophisticated data storage. Cloud storage mainly helps Small and Medium scale Enterprises (SMEs) to reduce their investments and maintenance of storage servers. Users' data that are sent to the cloud have to be stored in the public cloud storage. Security for the stored data in the cloud is more important. Security is the top most issue in cloud storage. Data security can be ensured by the confidentiality parameter. This paper proposes a secured confidentiality technique named AROcrypt to ensure the security of data stored in the cloud storage.It also describes Security as a Service (SEaaS) in the cloud environment. Simulations were conducted using a security analysis tool. AROcrypt compares with existing confidentiality techniques like DES, 3DES and Blowfish. The proposed AROcrypt technique is based on the symmetric encryption algorithm. It uses the ASCII values to process the plain text into cipher text. The proposed technique provides better performance and good security when compared with existing confidentiality techniques.**

Keyword-Cloud Computing, Data Security, Cloud Storage, Encryption, Confidentiality, SEaaS

I. INTRODUCTION

Cloud computing is a distributed computing service, comprising varied components like hardware, software, networking and storage. Cloud service is obtained through Internet [1][2]. Services mainly provided by the cloud areSoftware-as-a-Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) [3]. The primary usage of cloud computing services isdata storage [4]. Cloud storage has to be secured to keep the data safe. Cloud is a public environment where there are many possibilities to hack the user's data. Cloud security is the crucial part which deals with the issues and vulnerabilities of cloud computing for guaranteeing safer computing environment.

Security is a major challenge in cloud system due to its nature of outsourced computing [5][6]. Unless robust security scheme is implemented, cloud system will be vulnerable to various attacks and susceptible by the users. Data security is ensured by a number of different security parameters via Authentication, Authorization, Confidentiality, Integrity and Availability [7]. Mostly, confidentiality, integrity and authentication are the critical areas. Among these security parameters, this paper uses confidentiality parameter to ensure the security of data in the cloud storage. Confidentiality ensures that the data can be accessed only by the privileged cloud users.

Confidentiality is used to protect the data from the attack of outsiders and insiders.Cloud data may be attacked in two different ways [8]. One is outsiders' attack, and the other is insiders' attack. Outsiders are hackers'attack data from outside CSP. Insiders as administrators have the possibility to hack the user's data. Insider'sattacks are very difficult to identify. So the users must be very suspicious while storing their data in cloud storage. Even though the data is accessed by a third party, they could not get the actual data. So, all the data must be encrypted in cloud storage. There arevarious confidentiality techniques that are already used for data encryption. However, for the cloud environment, it needs more sophisticated technique to ensure security of data in the cloud. This paper proposes such a technique called AROcrypt.To prove the confidentiality of AROcrypt, it is compared with variousexisting techniques like DES, 3DES and Blowfish [9][10][11].

Cryptography [12] is a technique used for encryption and decryption. There are several cryptography techniquesavailable for encryption and decryption. Cryptographic techniquesareclassified into Conventional and Public key cryptography. Conventional cryptography is also referred as symmetric key encryption. The same key is used for encryption and decryption. Public key cryptography is called asasymmetric key encryption.The original intelligible message referred to as plain text is converted into apparently random ambiguous message referred to as cipher text. The encryption is a process comprises of an algorithm and a key.Choice of the key affects the results of the encryption algorithm.According to Tim Mather, [4] symmetric encryption is more suitable to handling encryption at minimum time and efficientfor large volumes of data in cloud storage.

Data security is a precarious issue in cloud computing environments. Cloud has no border, and the data can be physically located anywhere in any data centers across the geographically distributed network. So, the nature of cloud computing increases serious issues concerning user data confidentiality. Hence, it is needed to proposeand implement novel security technique to enhance the data security [13]. This paper proposes a confidentiality technique for SMEs to ensure security of data in cloud storage.

II. SECURITY AS A SERVICE (SEAAS)

Cloud computing provides Anything as a Service (XaaS). SEaaS is one of the services provided by the Cloud Service Provider (CSP). SEaaS provides different security service algorithms for securing the data in the cloud. Figure 1 shows the cloud environment with CSP, which has SEaaS as one of its services. CSPs provide many services like SaaS, PaaS and IaaS. Securityis also provided as a service. In figure 1, CSP_1provides SEaaS and also provides other services. Here, CSP_1 is used only for security service,and not for storing the data. Users could store their data with other CSPswho provide storage as a service.

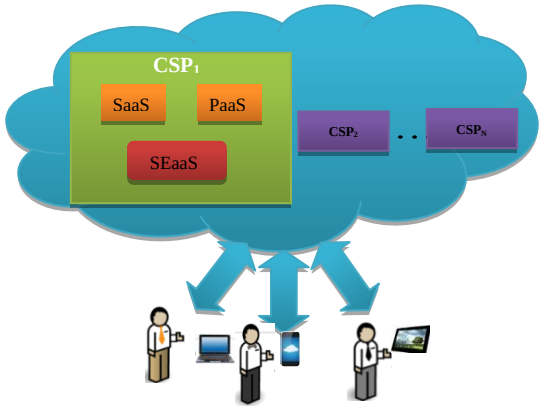

Fig1.CSPwith Security as a Service (SEaaS)

SEaaS contains three security service algorithms namely AROcrypt, MONcrypt and AROMONcrypt. These algorithms are particularly used for a specific type of data. If users want to upload any sensitive data to the cloud, they may use any one of the algorithms from SEaaS. Figure 2 represents the security services provided by SEaaS in a CSP. AROcrypt security service algorithm is used for non-numerical data. MONcrypt security service is used for numerical data. AROMONcrypt security service is used for numerical as well as non-numerical data. This paper only describesAROcrypt security service in SEaaS.

The users need not encrypt all the data uploaded to the cloud. Instead, they can encrypt only sensitive data. SEaaS is provisioned to the users to encrypt the sensitive data. Sensitive data may be numerical or non-numerical or both. AROcrypt technique is used to encrypt sensitive data of non-numerical type. Users should choose this technique when they upload non-numerical sensitive data. If users upload combination of numerical and non-numerical data, the AROcrypt encrypts only non-numerical data, and the other types of data are left as they are.

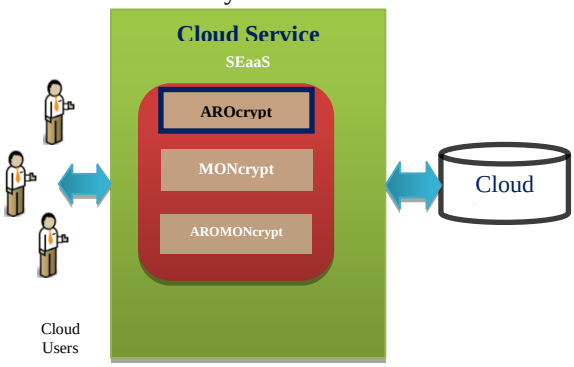

Fig. 2. Cryptography Technique provided by SEaaS

III. RELATED WORK

This section describes some of the related works already done in the field of cloud security. Seny k et al. [14] considered a problem to build securedcloud data storage for public cloud. This paper describes an architecture that consists of four components namelya data processor (DP), a data verifier (DV), a token generator (TG), and a credential generator(CG). Architecture is designed for both consumer and enterprises. This paper does not describe the key sharing technique and the client has maximum burden to maintain the components in the architecture.

Sunitha rani et al. [15] proposed an encryption algorithm in order to provide security in the cloud. The proposed methodology used three encryption algorithms sequentially to encrypt a message. First, plaintext is encrypted by the ceaser cipher. Then the encrypted result from ceaser cipher is again encrypted via using RSA substitution algorithm and finally the result from RSA is once again encrypted by the monoalphabetic substitution method**.** This technique has taken more time to encrypt the text by three algorithms one by one.

Subhasri P. et al. [16] proposeda Multi-level Encryption algorithm to secure the data in the cloud. The proposed algorithm uses rail fence and ceaser cipher algorithm. Initially, plaintext is encrypted using rail fence technique. Assign the position value i to each letter in the encrypted text.Generate the ASCII valuesof eachcharacter.Assign a key and apply it on the text using the formula: E = (p + k + i) % 256, where pdenotes Plaintext, k denotes key and i denotes Position. Algorithm produces the ASCII character of the equivalent decimal value.Key used for encryption is not generated. Maintain the position of each character in the text requiringadditional storage.Here, Author has not mentioned where the characters position details are maintained.

Yau SS et al. [17]presentedan approach to secure the users' data from service providers. This approach contains three mainparts: 1) separating software service providers, and infrastructure service providers, 2) hidingdata owner's information and 3) data obfuscation.

Manpreet K et al. [10]presentedaCipher Cloud framework. It helps users to keep their data confidential on public cloud. To achieve this, the framework uses a two-step encryption process, bywhich all the data sent from the client to cloud and cloud to client is retainedcompletely encrypted. A thorough security control is needed to protect the most sensitive data that may not be guaranteed in the public cloud computing architectures.

Anshu P et al. [9] proposed encryption algorithm to make cloud data secure and vulnerable. Author discusses security issues, challenges of cloud and comparesthe existing algorithms like AES, DES, BLOWFISH and RSA Algorithms.Comparison shows that DES algorithm consumes less encryption time. RSA takes larger memory usage and encryption time. AES algorithm takes less time to execute cloud data. Blowfish algorithm consumes minimum memory. Among these algorithms DES, 3DES and Blowfish are preferred to compare with AROcrypt.

IV. Problem Definition

Cloud attracts SMEs by its fascinating characteristics and benefits. Besides the cloud benefits, it has number of issues related to security, scalability, reliability and data migration, etc. Security is the highest concern in the cloud environment[18]. Outsourced data to thecloud are kept by third party cloud storage providers. In this situation, data may be attacked from inside as well as outside the cloud. Listed below are the problems to be considered for cloud data outsourcing.

- Data sent to the cloud is warehoused in public cloud storage.
- Cloud storage is controlled and maintained by cloud providers.
- Users do not have the rights to control and monitor the data in the cloud storage and do not even know where the data is kept.
- Data may be mingled with other user's data in cloud storage.
- Outsourced data is stored as plaintext in cloud storage like Amazon S3 [4].
- Key management for each customer is more difficult for the cloud provider; the same key is used for all customer data. It will lead to the data protection issue. Security, Privacy, Confidentiality and Integrity can be put at risk.
- Potential improper use of database information may be done by the provider itself.

V. Motivation

SMEs are ready to adopt the cloud storage by outsourcing their IT requisite. However, due to the issues related to security of data in the cloud storage, the SMEs are hesitant to store their data in the cloud storage. Security is achieved by confidentiality parameter. Motivated by this fact, this paper aims to ensure the confidentiality of outsourced data by achievingthe following goals.

- To ensure that stored data in the cloud is only accessed by the data owner.
- To prevent the unauthorized access by encrypting data before they are uploaded to cloud storage.
- To encrypt sensitive non numerical data.
- To propose a confidentiality technique for SMEs to secure data storage.

VI. Methodology

Outsourcing the data to the cloud provides many benefits to SMEs. Data are outsourcedin encrypted form [19]. Figure 3 shows the working procedure of SEaaSsecurity services. There are three primary processes namely encryption, key generation and data storage. Three different CSPs provide these three tasks. Steps involved in SEaaS model in the cloud environment are as follows:

1. User chooses an encryption algorithm from SEaaS in a CSP.
2. SEaaS of CSP_1 instructs the KGMaaS in CSP_2 to provide keys to the user who choosesparticular algorithm from SEaaS. SEaaS sends the user related information to KGMaaS to forward the keys.
3. KGMaaS generates keys suitable for the selected algorithm by the user. Keys are directly communicatedto the user, not through CSP_1.
4. User applies the keys to AROcrypt algorithm to encrypt the data. Once the data is encrypted, it is uploaded to the cloud storage of CSP_3.

Figure 3 showsthe process of encryption, key generation and storage by CSP_1, CSP_2 and CSP_3 respectively. CSPs are independent to others. CSP_3 provides Storage as a Service

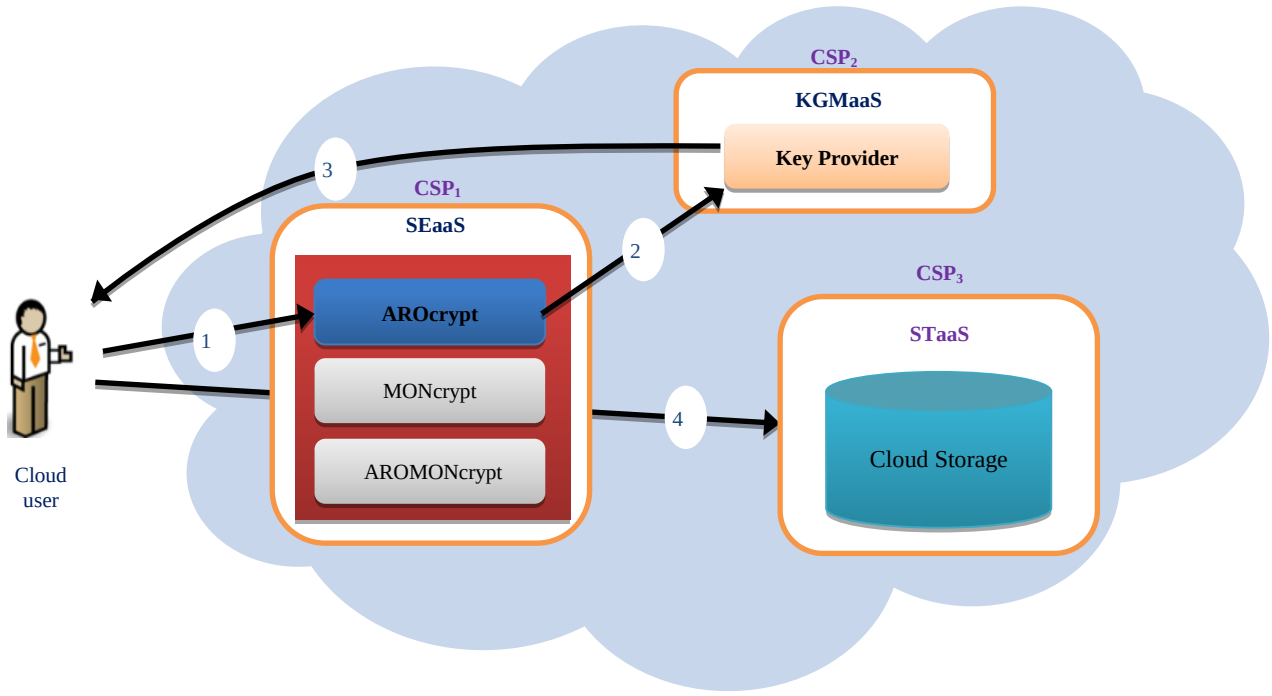

Fig. 3. SEaaS working procedure

(STaaS) to store customer data. CSP_2 has the key providing system and key management system. It maintains log table for key management. CSP_1 has SEaaS model to provide encryption algorithms for users to secure their data. The key used for encryption is kept by the user. If they want to share the uploaded data with their friends, they must send the key to their friend via secured channel.

VII. PROPOSED AROCRYPT TECHNIQUE

Cloud computing provides efficient storage setting to store and retrieve the cloud user's data. Ensuring data security is a vital role to cloud users as well as cloud providers. Proposed security serviceprocesses the data, and then data are submitted to the cloud storage. Data encryption is done by choosing AROcrypt security service algorithm by the user. The encryption key used for algorithm is receivedfroma CSP to the user.

Algorithm #1 shows the proposed AROcrypt security service algorithmin CSP_1. It is a symmetric encryption algorithm. It uses four keys for encryption and the same keys are used for decryption. The given plain text characters are converted into ASCII values. A square matrix is formed based on the number of characters in the plaintext. Maximum size of the matrix is 25_X25. The square matrix is divided into three matrices called upper (*UMAT*), diagonal (*DMAT*) and lower (*UMAT*) matrix. Apply the encryption to the matrices *UMAT*, *DMAT* and *UMAT* individually by using the keys K_1, K_2, K_3respectively. Another square matrix is constructed with an encrypted value. Nowthe text is read column by column.Order of understanding the column is based on order of Key K_4. Finally, the ASCII code values are converted intocharacter value.This value is ciphertext.

Algorithm #1: AROcrypt Security Service Algorithm

1. encryption_text(T)
2. start
3. Convert (T) into ASCII code
4. N= count (T)
   // N- number of characters in T
   //form the matrix for N character, maximum size of matrix is 25X25, if N>625 than divide the T into 625 character blocks and form matrix for each block.
5. matc =N/625
6. if matc>0
   fori=1 to matc
   Divide the T into 625 blocks, N=n_1, n_2, n_3…n_n// n_1, n_2, n_3 are each individual matrix
   end loop
   end if
7. for p=1 to matc
8. Based on the value of N, form a square matrix MAT [MXM] > N,M=M
9. Apply T into the matrix from left to right
10. Divide the Matrix MAT into three matrices called UMAT,DMAT,LMAT
    //UMAT-Upper Matrix, DMAT-Diagonal Matrix, LMAT-Lower Matrix
11. Read the Text T by UMAT(U), DMAT(D) and LMAT(L)matrix
    //U, D, L- text of upper, diagonal and lower matrix respectively
    // generate the random number for keys
12. Get three random integer number as KEYS K_1, K_2, K_3 for each matrix.
13. Apply the key K_1, K_2, K_3 for U, D, L to get first encrypted data
    // [U-K_1, D-K_2, L-K_3]
14. Arrange the encrypted text into another matrixMAT_1 [MXM]based on number character in the key K_4
15. Read the matrix MAT_1 column by column in order of key K_4
16. Resultant text from step 15 is converted to ASCII character code(C)
    //C-Cipher Text
17. end loop
18. end

Algorithm #2 is used for the generation of random integer number from CSP_2. This algorithm generates a random value. CSP_1 instructs CSP_2 to generate three integers valued key for K_1, K_2 and K_3 and one string key for k_4. These four keys are forwarded to the cloud user directly by CSP_2.

Algorithm #2: Random Number Generation

1. intrandom_num_gen()
2. start
   // generation of random using random() class
3. ran=new random().nextInt(100)
4. return ran
5. end

The proposed AROcrypt security service algorithm is applied on the non-numeric type of data. AROcrypt ensures the confidentiality of cloud data. It can protect the data in cloud storage from insiders and outsiders attacks. The key used for encryption is kept by the cloud user, so the cloud storage provider does not have any knowledge about the key because the key is not communicated to them. Cloud users do not have any work burden to encrypt the data with AROcrypt. The hacker (insider or outsider) may get the encrypted data stored in the cloud, but they could not get a clear understanding about the data. It increases the confidentiality of the data stored in the cloud storage.

VIII. SIMULATION RESULTS

The proposed AROcrypt technique and key generation is implemented in JAVA. Simulation is performed in the cloud environment (Amazon EC2). The cloud user machine connected to the cloud server has the configuration of Windows Operating System with core i3 Intel processor and 4GB RAM. The user data are encrypted before it is uploaded and decrypted when it is retrieved from the cloud. Thus, the encryption is done in the user machine connected to the cloud. Time taken for encryption and decryption is calculated in the user machine.

Amazon Elastic Compute Cloud (EC2) server is used for cloud storage. Key generation and AROcrypt techniques are developed as web service and hosted in the Amazon server. The Amazon micro instance has the following

configurationasMicrosoft windows server 2008 Base 32 bit operating system, 2.5 GHz Intel xeon processor, 613 MB RAM, 30GB of EBS (Elastic Block Storage). The users upload the data via user interface. Once the data are submitted, then they are encrypted and uploaded to the Amazon micro instance server. Security levels of the existing and proposed techniques are computed in Amazon server.

Security level is analysed by using a security analysis tool called Hackman. This tool analyses the security level of proposed and existing techniques. This tool is installed in Amazon server for analysing the security level of each technique. Hackman attacks the encrypted text in the Amazon server. It uses different attacks like dictionary attack, brute force attack, etc. to retrieve the original text. Map the plain text with retrieved text to find the percentage of original text retrieval. Based on percentage mapping, security level of the proposed technique is estimated. In the same way, existing cryptography techniques security level are calculated and compared with the proposed technique.

Performance and security level of proposed AROcrypt technique is compared with existing encryption techniques. Time taken for encryption and decryption is shown in Table 1 and Table 2 respectively. Security levels of proposed and existing techniques are compared and shown in Table 3. Simulation is conducted for different sizes of data. For each size of data, time taken for encryption, decryption and security level are noted and evaluated with existing techniques. Performance of proposed technique is measured by the time taken to complete encryption and decryption process.

TABLE I. Performance Comparison based on Encryption Time (Milliseconds)

Size	Encryption Techniques			
	DES	*3DES*	*Blowfish*	*AROcrypt*
1 MB	502	618	397	282
2 MB	967	1078	602	468
3 MB	1302	1422	891	656
4 MB	1701	1847	1073	889
5 MB	2108	2236	1207	1102
10 MB	4282	4404	2421	2253
15 MB	6331	6597	3642	3388

Table I represents the time taken for encrypting the data using proposed AROcrypt and existing techniques like DES, 3DES and Blowfish.

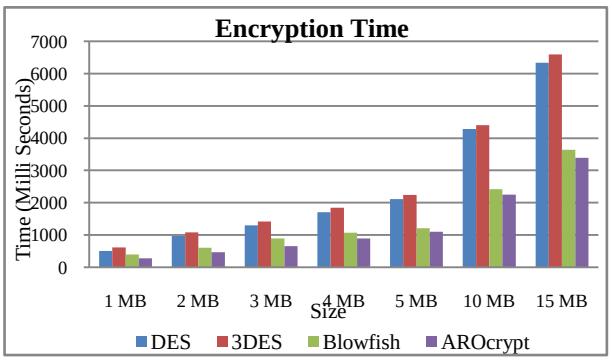

Fig.4.Performance Comparison based on Encryption Time

Table I and Figure 4 represent the performance comparison of proposed AROcrypt encryption algorithm with existing algorithms. The time taken by the existing and proposed encryption algorithms are calculated for different sizes of data. The result shows that the proposed AROcrypt algorithm has taken minimum time duration for encrypting the data of different sizes when compared to the existing algorithms.

TABLE II.PERFORMANCE COMPARISON BASED ON DECRYPTION TIME (MILLISECONDS)

Size	Decryption Techniques			
	DES	*3DES*	*Blowfish*	*AROcrypt*
1 MB	497	607	312	235
2 MB	958	1062	592	438
3 MB	1289	1403	837	627
4 MB	1689	1832	996	843
5 MB	2084	2219	1170	1069
10 MB	4116	4391	2231	2216
15 MB	6298	6578	3512	3341

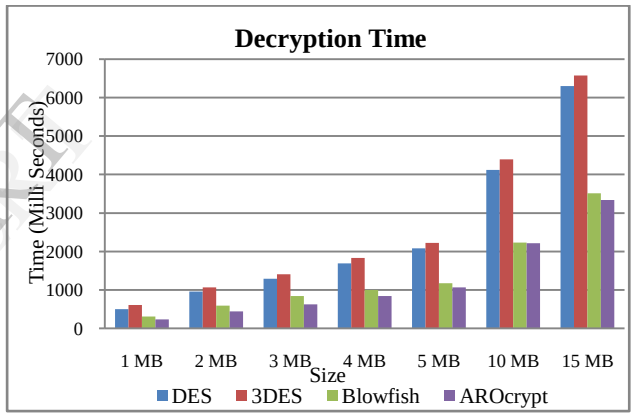

Fig. 5.Performance Comparison based on Decryption Time

Table II and Figure 5 represent the performance comparison of decryption with existing techniques. The time taken by the existing and proposed decryption techniques are calculated for different sizes of data. The result shows that the proposed AROcrypt technique has taken minimum time duration for decrypting the data of different sizes when compared to the existing techniques.

TABLE III.COMPARISON OF SECURITY LEVEL

S.No	Techniques	Security Level (%)
1.	DES	74
2.	3DES	82
3.	Blow fish	78
4.	AROcrypt	89

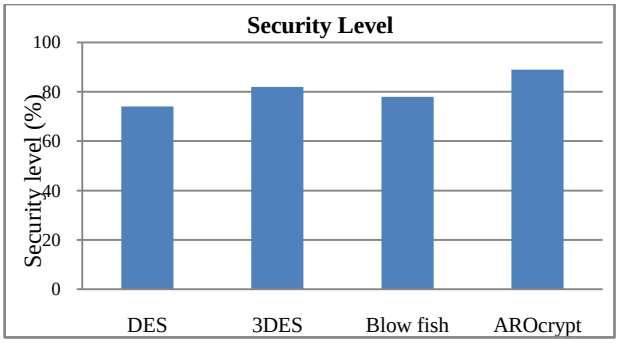

Fig.6. Comparisonof Security Level

Table III and Figure 6 represent the comparison of security level based on the security analysis tool. The result shows that the proposed AROcrypt technique secures 89% of security that is higher than the existing techniques.

The above results show that the AROcrypt technique gives maximum security and better performance than existing techniques while storing the data in the cloud. Hence, the confidentially of the data stored in the cloud is achieved.

IX. Conclusion

Cloud Storage is a cost-effective IT service to the general user or enterprise customer. Most of SMEs do not have the infrastructure to keep their data safe. Cloud storage provides plenty of storage capability with nominal cost. SMEs are interested in outsourcing their sensitive data to the cloud storage. However, there are some security problems with cloud storage.Due to this, enterprises are disinclined to use the cloud. Once the issues are resolved, cloud computing would be a trillion dollar business in the computing world. Data storage on un-trusted cloud creates data security as a challenging problem. The confidentiality parameter ensures data security in the cloud. This paper proposed a new cryptographic technique named AROcrypt to address the security problems in cloud storage. This AROcrypt technique is provided through SEaaS model. Encrypted data are stored on storage server while secret keys are retained by data owner and access to the user is granted by issuing the corresponding decryption keys. AROcrypt technique is based on a symmetric encryption technique. The data are encrypted before they are forwarded to the cloud storage. Hence, in this paper a new confidentiality technique has been proposed and implemented. Simulation results show the comparison of AROcrypt with existing techniques. From the results, it is observed that AROcrypt technique offers better performance and maximum protection to the data stored in the cloud than the existing encryption techniques.

References

[1] Arijit, U., Debasish, J. and Ajanta, D.S., A security framework in cloud computing infrastructure, International Journal of Network Security & Its Applications (IJNSA), Vol. 5, pp. 11-24, 2013.

[2] John, H., L.M. Kaufman and Bruce, P., "Data security in the world of cloud computing" IEEE Security & Privacy, pp. 61-64, 2009.

[3] Kelsey Rauber, "Cloud Cryptography", International Journal of Pure and Applied Mathematics, Vol. 85, pp. 1-11, 2013.

[4] Mather T., Kumaraswamy S. andShahed, L., "Cloud security and privacy", Chapter 4, O'Reilly Media, Inc, pp. 61-71, 2009.

[5] Xiaojun, Y. and Qiaoyan, W., "A view about cloud data security from data life cycle", IEEE International Conference on Computational Intelligence and Software Engineering (CiSE), pp. 1-4, 2010.

[6] Abhishek, P and Mayank, K., "A proposed model for data security of cloud storage using trusted platform module", International Journal of Advanced Research in Computer Science and Software Engineering,Vol3,pp. 862-866, 2013.

[7] Arockiam L., Monikandan S, and Sheba K Malarchelvi P. D., "Obfuscrypt: A Novel Confidentiality Technique for Cloud Storage", International Journal of Computer Applications, Vol. 88, pp. 17-21, 2014.

[8] Arockiam, L and Monikandan, S., "Data security and privacy in cloud storage using hybrid symmetric encryption algorithm", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, pp. 3064-3070, 2013.

[9] AnshuParashar and RachnaArora, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications, Vol. 3, pp. 1922-1926, 2013.

[10] ManpreetKaur and Rajbir Singh, "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", International Journal of Computer Applications, Vol. 70, pp. 16-21, 2013.

[11] RashmiNigoti, ManojJhuria andDr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing", International Journal of Emerging Technologies in Computational and Applied Sciences, Vol4, pp. 141-146, 2013.

[12] William, S., "Cryptography and network security: principles & practices", Fifth edition, Prentice Hall, pp. 6-56, 2005.

[13] Sudha M., Monica M., "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography", Advances in Computer Science and its Applications, pp. 32-37, 2012.

[14] Kamara S. andLauter K., "Cryptographic cloud storage", IFCA/ LNCS 6054, Springer-verlag, Berlin Heidelberg, pp. 136-149, 2010.

[15] Sunita Rani, AmbrishGangal "Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints", International Journal of Computer Science and Information Technologies, Vol.3, pp.4302–4304, 2012.

[16] Subhasri P., Padmapriya A., "Multilevel Encryption for Ensuring Security in Public Cloud", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, pp. 527-532, 2013.

[17] Yau SS, An HG. "Confidentiality protection in cloud computing systems", International Journal Software Informatics, Vol.4, pp. 351-365, 2010.

[18] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan and BhavaniThuraisingham, "Security Issues for Cloud Computing", International Journal of Information Security and Privacy, Vol.4, pp. 39-51, 2010.

[19] Atiq, U.R. and M. Hussain, "Efficient cloud data confidentiality for DaaS", International Journal of Advanced Science and Technology, Vol.35, pp. 1-10, 2011.

[20] Isaac Agudo, David Nuñez, Gabriele Giammatteo, PanagiotisRizomiliotis andCostas mbrinoudakis, "Cryptography Goes to the Cloud", Communications in Computer and Information Science, Springer-verlag, Berlin Heidelberg,Vol.187, pp. 190-197, 2011.

[21] Sascha, F., Marian, H., Thomas, M and Matthew, S., "Confidentiality as a service – usable security for the cloud", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 153-162, 2012.