Appendices
Appendix - i

Papers Published in the International Journals
Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm

Dr. L. Arockiam¹, S. Monikandan²
Associate Professor, St. Joseph’s College, Trichy, Tamilnadu, India²
Research scholar, M S University, Tirunelveli, Tamilnadu, India²

Abstract — One of the primary usage of cloud computing is data storage. Cloud provides enormous capacity of storage for cloud users. It is more reliable and flexible to users to store and retrieve their data at anytime and anywhere. It is an increasingly growing technology. Nowadays, many enterprises have started using cloud storage due to its advantages. Even though the cloud continues to gain popularity in usability and attraction, the problems lie in data security, data privacy and other data protection issues. Security and privacy of data stored in the cloud are major setbacks in the field of Cloud Computing. Security and privacy are the key issues for cloud storage. This paper proposes an encryption algorithm to address the security and privacy issue in cloud storage in order to protect the data stored in the cloud.

Keywords: Cloud Storage, Security, Privacy, Encryption Algorithm, Cryptography

I. INTRODUCTION

Cloud is a technology invention. It provides the computational resources (Server, Storage, OS and Network) to user as service based on demand. Cloud computing has emerged as a popular solution to provide cheap and easy access to externalized IT (Information Technology) resources. An increasing number of organizations (e.g., research centres, enterprises) benefit from Cloud computing to host their applications [1]-[2]. Virtualization is the core concept supported in the cloud computing. Resources are provided to cloud users as virtualized manner [3]. Virtualization and cloud computing can be used quite successfully to improve the resilience of an IT environment. Because, they provide the means to recover quickly from component or system malfunctions using failover. Quickly take back up of essential applications and data. Virtual machines can be migrated from one physical server to another in a live migration; virtual machine images can be restarted in a different location to provide for disaster recovery [4].

Cloud has three types of services. They are Software as a service, Platform as a service and Infrastructure as a service. Cloud services are provided by the different cloud providers like Amazon, Google, Microsoft, IBM and etc. The users can utilize these services (SaaS, PaaS and IaaS) based on their requirement. Usage of these three services, user’s data are stored in the cloud storage. Cloud providers are maintaining the user’s data in cloud environment. The data in the provider’s hands could make security and privacy issue in cloud storage. With cloud computing, all users’ data are stored on the cloud. So cloud users have to think about their data [5] like: security of the data in the cloud, Access control and authentication of the cloud. Cloud computing companies say that data is secure, but it is too early to be completely sure of. Only time will tell if user’s data is secure in the cloud.

Cloud security and privacy concerns are arising in which both customer’s data and application are residing in provider’s premises. Security and privacy are always a major concern in cloud computing [6]-[7] as shown in Fig.1. It shows the survey report of 2008 and 2009 by International Data Corporation (IDC). From the figure, it is clear that security is the top most concern in cloud computing in the survey of both years.

While cost and ease of use are two great benefits of cloud computing [5], there are significant security concerns that need to be addressed while moving critical applications and sensitive data to public and Cloud storage. Cloud data may be attacked in two ways. One is outsider attack and the other is insider attack. Insider as an administrator can have the possibility to hack the user’s data. Insider attack is very difficult to be identified. So the users should be very careful while storing their data in cloud storage. Even though the data is accessed by the third party, they shouldn’t get the actual data. So, all the
data must be encrypted before it is transmitted to the cloud storage. Cryptography is a technique applied for encryption and decryption. In the field of cryptography there are several techniques available for encryption/decryption. These techniques can be generally classified into two major groups, i.e. Conventional and public key Cryptography [8]. Conventional cryptography is also referred as symmetric encryption or single key encryption. Same key is used for encryption and decryption. Public key cryptography is referred as asymmetric encryption or public key encryption. Separate keys are used for encryption and decryption. Fig.2 represents the simplified model for conventional encryption technique. The original intelligible message, referred as plaintext, is converted into apparently random ambiguous message, referred as ciphertext. The encryption process consists of an algorithm and a key. The key is a value independent on the specific of the plain text. The algorithm will produce a different output depending on the specific key being used at that time. Changing the key changes the output of the algorithm. Once the ciphertext is produced, it may be transmitted to cloud storage. Upon reception, the ciphertext can be transformed back to the original plaintext by using a decryption algorithm with the same key that was used in encryption.

This paper proposes a symmetric encryption algorithm to protect the user’s data stored in the cloud storage from the unauthorized access. The paper is organized as follows. Section II gives the detail on the various issues in cloud data storage. Section III describes the symmetric encryption algorithm and how it is executed. Section IV talks about the different classical encryption algorithms that are already used in the data security. In Section V, proposed encryption and decryption algorithm are described in detail. Section VI gives the conclusion for the paper.

II. ISSUES IN CLOUD DATA STORAGE
Cloud Computing moves the application and data to the cloud storage, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. This paper focuses on cloud data storage security, which has always been an important aspect of quality of service. Following are the issues [10] in cloud data storage.

A. Privacy
Different from the traditional computing model, cloud computing utilizes the virtual computing technology. User’s personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders. At this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depending on the computing task submitted by the users. The major privacy issues [11] relate to i) Trust, i.e. whether there is unauthorized secondary usage of PII (Personally Identifiable Information), ii) Uncertainty, i.e. ensuring that data has been properly destroyed by the one who controls retention of data on how the privacy breaches have occurred and how the fault is determined in such cases iii) Compliance, i.e. environments with data proliferation and global, dynamic flows, and addressing the difficulty in complying with transborder data flow requirements.

B. Security
Security concerns relate to risk areas such as external data storage, dependency on the public internet, lack of control, multi-tenancy and integration with internal security [12]. Cloud service providers employ data storage and transmission encryption, user authentication, and authorization. Many clients worry on the vulnerability of remote data to hackers. Cloud providers are enormously sensitive to this issue and apply substantial resources to mitigate this problem.

C. Trust
Trust issue in cloud computing has equal concern against security and privacy. Trust is defined as reliance on the integrity, strength, ability and surety of a person or thing. Entrusting user data on to a third party who is providing cloud services is an issue. For example, in April 2012, Amazon's Elastic Compute Cloud service crashed during a system upgrade, knocking customers' websites off-line all over for several hours for several days. Another incident happened on the same month. The hackers broke into the Sony PlayStation Network, exposing the personal information to 77 million people around the world. These issues have certainly created doubts in mind of cloud users and damaged the trust [10].

D. Ownership
Once data has been submitted to the cloud, developers have concern about losing their rights or being unable to protect the rights of their customers. Many cloud providers address this issue with well-skilled user-sided agreements.
According to the agreement, users would be wise to seek advice from their favourite legal representative.

E. Performance and Availability

Business organizations are worried about acceptable levels of performance and availability of applications hosted in the cloud. Application and data in the cloud storage should be available to the users at anytime and anywhere. Users have no worry about the local system which is used for accessing the cloud servers.

F. Long-term Viability

Users should be sure that the data put into the cloud will never become invalid even the cloud computing provider get lost or get acquired and swallowed up by a larger company. Users should ask their potential providers of cloud how they would get user’s data back and if it would be in a format that user could import into a replacement application [13].

H. Data Backup

Cloud providers employ redundant servers and routine data backup processes, but users worry about being able to control their own backups. Many providers are now offering data dumps onto media or allowing users to back up data through regular downloads.

G. Data Portability and Conversion

Users have concerns on data portability like, switching between service providers. There may be difficulty in transferring data. Porting and converting data is highly dependent on the nature of the cloud provider’s data retrieval format, particularly in cases where the format cannot be easily revealed. As service competition grows, open standards become established, the data portability issue will ease, and conversion processes will become available supporting the more popular cloud providers. Worst case is that the cloud subscribers have to pay for some custom data conversion.

These are certain areas in which cloud computing requires to excel and solve problem related to it. Out of all the problems; narrated Security and Privacy [14] put the major threats in growth of cloud computing. It needs to be worked upon.

III. SYMMETRIC ENCRYPTION

Symmetric encryption (see Fig.2) involves the use of a single secret key for both the encryption and decryption of data. Only symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data [9].

For example, a source produces a message in plaintext, \( X = \{X_1, X_2, X_3, \ldots, X_M\} \). For Encryption, a key is generated at the message source. Then the key is also provided to the destination by means of some secure channel. With the message \( X \) and the encryption key \( K \) as input, the encryption algorithm forms the cipher text \( Y = \{Y_1, Y_2, \ldots, Y_N\} \). This may be written as \( Y = E_K(X) \).

Cipher text \( Y \) is produced by using encryption algorithm, where \( E \) indicates the encryption algorithm used and \( K \) indicates the key used for encryption. The receiver of this message should apply decryption algorithm with same key used for encryption to get the actual message \( X = D_K[Y] \). Here \( D \) indicates decryption algorithm.

IV. CLASSICAL ENCRYPTION

Several encryption algorithms are available and are used in information security. These algorithms can be categorized as classical encryptions [15]. These encryption algorithms are based on two general principles namely substitution cipher, in which each element in the plaintext is mapped into another element, and transposition cipher, in which elements in the plaintext are rearranged. Out of the different encryption algorithms, few algorithms are described in this section.

A. Caesar Cipher

Caesar cipher [16] is a classical substitution cipher and it is one of the simplest examples of substitution cipher. It replaces alphabet of letter in the plain text, with a letter 3 places ahead of it. For example, “HELLO” is a plain text which will be converted into “KHOOR” as cipher text. One can see that such a cipher may be difficult to break. This cipher can be broken by brute force attack because at the end there are only 25 possible available options of key.

B. Playfair Cipher

Another example of classical substitution cipher is Playfair cipher [17] which has a square matrix of 5X5 alphabetical letters arranged in an appropriate manner. The user can select a key and place it in the matrix. The remaining letters of English alphabet from the key are then one by one placed in the matrix of Playfair cipher. The plain text is broken into pairs and if a pair has same alphabet then they are separated by introducing a filler letter with ‘x’. Otherwise if the pair is with different alphabetical letters and resides in the same row of matrix then each letter is replaced by the letter ahead of it. If the pair of letters is in same column of matrix then each letter is replaced by the letter below it, and when the pair of letters is neither in same column nor in same row then they are replaced by the letter in their row that resides at the intersection of paired letters.

C. Vigenere Cipher

Vigenere cipher [18] when compared with Caesar cipher gives some level of security with the introduction of a keyword. This key word is repeated to cover the length of the plain text which is to be encrypted. Example is shown below:

\[
\begin{align*}
\text{KEY} & : f a u z a n f a u z a n \\
\text{Plain text} & : c r y p t o g r a p h y \\
\text{Cipher} & : H R S O T B L R U O H L
\end{align*}
\]

As it can be seen that above example, “fauzan” is a keyword and plain text is “cryptography” which is
encrypted into “HRSOTBLROUHL”. This is done using Vigenere table which contains alphabets in form of rows and columns left most column. The left most column indicates keyword and top most row indicates plaintext and at the junction of two alphabetical letters resides our replacement. After individually transforming every letter, user gets an encrypted message.

D. Rail fence technique
This is one of the transposition ciphers [8], in which the plain text is written down as a sequence of diagonal and then read as a sequence of rows. For example, to encipher the message “hai welcome” with a rail fence of depth 2,

\[
\begin{array}{cccc}
hi & ec & m \\
aw & lo & e
\end{array}
\]

Now the encrypted message is “hiecmawloe”. In this technique the same alphabets in the plaintext is rearranged. This technique alone cannot be sufficient for data security.

V. PROPOSED ALGORITHM
Proposed technique emphasizes on improving classical encryption techniques by integrating substitution cipher and transposition cipher. Both substitution and transposition techniques have used alphabet for cipher text. In the proposed algorithm, initially the plain text is converted into corresponding ASCII code value of each alphabet. In classical encryption technique, the key value ranges between 1 to 26 or key may be string (combination alphabets). But in proposed algorithm, key value range between 1 to 256. This algorithm is used in order to encrypt the data of the user in the clouds. Since the user has no control over the data after his session is logged out, the encryption key acts as the primary authentication for the user. Proposed algorithm is described below.

A. Encryption Algorithm
Followings are the steps in proposed encryption algorithm.

**Encryption Algorithm:**

step 1. Count the No. of character (N) in the plain text without space.
step 2. Convert the plain text into equivalent ASCII code.
step 3. Form a square matrix \((S \times S >= N)\).
step 4. Apply the converted ASCII code from left to right in the matrix. Divide matrix into three parts namely upper, diagonal and lower matrix.
step 5. Read the value from right to left in each matrix.
step 6. Each matrix use three different key \(K_1, K_2, K_3\) for encryption. Do the encryption.
step 7. Apply the encrypted value into the matrix in the same order of upper, diagonal and lower.
step 8. Read the message by column by column. Here the order in the columns read from the matrix is the key \(K_4\).

The followings are the detailed description of each step in the proposed encryption algorithm.

**Step 1:**- Count No. of characters (N) in the message without space.

Plaintext - HIHOWAREYOU.

\[N=11\text{ (N = No. of Characters in the Message)}\]

**Step 2:**- Convert the plain text into equivalent ASCII code. And form a square matrix.

ASCII code value for the plaintext:

<table>
<thead>
<tr>
<th>72</th>
<th>73</th>
<th>79</th>
<th>87</th>
<th>65</th>
<th>82</th>
<th>69</th>
<th>89</th>
<th>79</th>
<th>85</th>
</tr>
</thead>
</table>

To form a square matrix, choose a number \((S)\), square value of \(S\) is immediately next to \(N\). i.e. \(S^2\) is nearest square value \(N\) and \(S^2 \geq N\).

For this plaintext \(N=11\), so \(S=4\).

The order of matrix is \(4 \times 4 = 11\), Form a \(4 \times 4\) matrix.

**Step 3:**- Apply the converted ASCII code message row by row in \(S \times S\) matrix. Separate the matrix into three parts as Upper, Diagonal and Lower. Following shapes represent the upper, diagonal and lower matrix position in the square matrix.

- Upper - diagonal - Lower

\[
\begin{array}{cccc}
72 & 73 & 79 & 65 \\
87 & 89 & 66 & 67 \\
68 & 69 & 65 & 67 \\
\end{array}
\]

**Step 4:**- Read the message from left to right for upper, diagonal and lower.

\[
\begin{array}{cccc}
72 & 73 & 72 & 79 \\
87 & 65 & 82 & 69 \\
89 & 79 & 85 & 65 \\
66 & 67 & 68 & 69 \\
\end{array}
\]

The values of three matrixes are,

- Upper Matrix - 73 72 89 85
- Diagonal - 65 82 67 68
- Lower matrix - 72 89 66 67

**Step 5:**- To encrypt the message use three different keys for upper, diagonal and lower matrix separately. Keys are \(K_1\) for upper matrix, \(K_2\) for diagonal matrix and \(K_3\) for lower matrix.

Upper Matrix = 23 -- \(K_1\)
Diagonal Matrix = 17 -- \(K_2\)
Lower Matrix = 6 -- $K_3$

Now add this key value with ASCII code message of each matrix.

After Encryption:
Upper Matrix = - 96 95 102 105 92 88
Diagonal = - 89 82 102 86
Lower matrix = - 93 95 85 72 73 74

**Step 6:** Apply the message into the square matrix in the same order of how it was read.

```
4   2   1   3 Key- K_4
| 89 96 95 102 |
| 93 82 105 92 |
| 95 85 102 88 |
| 72 73 74 86 |
```

**Step 7:** Now Read the message from the matrix by column by column. Here the order of the columns read in the matrix is the key $K_4$.

```
 89 96 95 102
93 82 105 92
95 85 102 88
72 73 74 86
```

**Step 8:** Covert the ASCII code into the equivalent character value. Then,

Encrypted cipher text is: _ifJRifXVY]_H

**B. Decryption Algorithm**

The encrypted data is stored in the cloud storage. To retrieve the data from cloud, decryption is necessary to get the actual data in the cloud. Decryption is possible only with key values which are used for encryption. So key should have a vital role in encryption and decryption algorithm. Following steps illustrate the decryption algorithm.

Decryption Algorithm:

**Step 1:** The encrypted text is converted into ASCII code values.

**Step 2:** Count the No. of character (N) in the decrypted text and form a square matrix $S 	imes S$.

No. of characters are $N=16$, so $S=4$, Order of matrix is $4 	imes 4$.

**Step 3:** Apply the ASCII code in the $S 	imes S$ matrix as column by column based on key $K_4$.

```
| 89 96 95 102 |
| 93 82 105 92 |
| 95 85 102 88 |
| 72 73 74 86 |
```

**Step 4:** Divide the matrix into upper, diagonal and lower.

Read the message in the matrices from left to right.

```
| 89 96 95 102 |
| 93 82 105 92 |
| 95 85 102 88 |
| 72 73 74 86 |
```

**Step 5:** Apply reverse encryption using the keys $K_1$, $K_2$ and $K_3$ on the upper, diagonal and lower matrix respectively.

Upper Matrix = 23 -- $K_1$
Diagonal Matrix = 17 -- $K_2$
Lower Matrix = 6 -- $K_3$

Decrypt the message using the keys. The values of three matrices after decryption.
Security and Privacy of data stored in Cloud Computing is an area which has full of challenges and of paramount importance. Many research problems are yet to be identified. Cryptographic techniques are used to provide secure communication between the user and the cloud. Symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data in cloud storage. This paper proposed a symmetric encryption algorithm for secure storage of cloud user data in cloud storage. The proposed encryption algorithm is described in detail and the decryption process is reverse of the encryption. This algorithm is used in order to encrypt the data of the user in the cloud. Since the user has no control over the data once their session is logged out, the encryption key acts as the primary authentication for the user. By applying this encryption algorithm, user ensures that the data is stored only in secured storage and it cannot be accessed by administrators or intruders.

VI. CONCLUSION

Security and Privacy of data stored in Cloud Computing is an area which has full of challenges and of paramount importance. Many research problems are yet to be identified. Cryptographic techniques are used to provide secure communication between the user and the cloud. Symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data in cloud storage. This paper proposed a symmetric encryption algorithm for secure storage of cloud user data in cloud storage. The proposed encryption algorithm is described in detail and the decryption process is reverse of the encryption. This algorithm is used in order to encrypt the data of the user in the cloud. Since the user has no control over the data once their session is logged out, the encryption key acts as the primary authentication for the user. By applying this encryption algorithm, user ensures that the data is stored only in secured storage and it cannot be accessed by administrators or intruders.

REFERENCE


BIography

Dr. Arockiam. L is working as Associate Professor in the Department of Computer Science, St.Joseph’s College (Autonomous), Tiruchirappalli, Tamil Nadu, India. He has 24 years of experience in teaching and 17 years of experience in research. He has published more than 140 research articles in the International / National Conferences and Journals. He has also presented 2 research articles in the Software Measurement European Forum in Rome. He has chaired many technical sessions and delivered invited talks in National and International Conferences. He has authored a book

S. Monikandan is working as Assistant Professor in Christuraj Institute of Computer Application, Christhu Raj College, Tiruchirappalli, Tamil Nadu, India. He is completed his MCA and M.Tech degree in Bharathidasan University, Tiruchirappalli in 2007 and 2009 respectively. Now, he is pursuing his research in Manonmaniam Sundaranar University, Tirunelveli. He has attended many International and National Conferences, Seminars and Workshops. His research interest is web technology and cloud storage security.
Obfuscrypt: A Novel Confidentiality Technique for Cloud Storage

L. Arockiam, Ph.D
Associate Professor,
St. Joseph’s College,
Trichy, India

S. Monikandan
Research Scholar,
M S University,
Tirunelveli, India

P. D. Sheba K Malarchelv, Ph.D
Professor & HOD of CSE,
JJ College of Eng & Technology,
Trichy, India

ABSTRACT
In today’s IT industry, the more sophisticated data storage is cloud storage. Cloud storage mainly helps Small and Medium scale Enterprises (SMEs) to reduce their investments and maintenance of storage servers. Most of SMEs are outsourcing their data to cloud storage. Users’ data that are sent to the cloud have to be stored in the public cloud environment. Data stored in the cloud storage might mingle with other users’ data. This will lead the data protection issue in cloud storage. If the confidentiality of cloud data is broken, then it will cause loss of data to the industry. Security of cloud storage is ensured through confidentiality parameter. To ensure confidentiality, the most commonly used technique is encryption. But encryption alone doesn’t give maximum protection to the data in the cloud storage. To have efficient cloud storage confidentiality, this paper uses encryption and obfuscation as two different techniques to protect the data in the cloud storage. Based on the type of data, encryption and obfuscation can be applied. Encryption can be applied to alphabets, alphanumeric and symbols. Obfuscation can be applied to numeric type of data. Applying encryption and obfuscation techniques on the cloud data will provide more protection against unauthorized usage. Confidentiality could be achieved with a combination of encryption and obfuscation.

Keywords
Cloud computing; Cloud Storage; Encryption; Obfuscation; Confidentiality;

1. INTRODUCTION
Cloud computing delivers massively scalable computing resources as a service with Internet based technologies. Resources are shared among a vast number of consumers allowing for a lower cost of IT ownership [1][2]. At present, cloud computing is widely discussed in academia and industry. With virtualization and distributed computing technology cloud computing integrates the computing, storage, networking and other computing resources, and then leases to users. Such mode could reduce the cost of enterprise information construction and accelerate the informatisation of enterprise. The Cloud storage is designed for virtualized computer environment. The cloud storage is implemented using cloud computing that means utilizing the software and hardware resources of the cloud computing service provider. Cloud computing is growing at a very high velocity in the IT industry around the world. While there are many advantages of cloud computing, the some enterprises are still waiting to use cloud computing. Hence the data security problem of cloud computing is not solved completely. Cloud Storage provides a virtual space to store bulk data. But the data owners have no control over their data. The cloud provider has full control on the user’s data. This makes the user’s mind to think about the data security in the cloud.

Data protection in the cloud storage is the core security problems. Data protection [3] is concerned with data confidentiality, integrity, authentication, availability and so on. Data confidentiality means that only authorized persons can use the data. Data integrity refers to information that has not been modified or remains untouched. Authentication refers to the process of verifying whether the incoming user is authorized or not. Data availability refers to the ability to guarantee to use data in time when needed and also refers to the availability of cloud service provider on-demand.

Figure 1 represents the layers of data security in the cloud. First layer is availability, which ensures the availability of cloud computing resources or availability of the cloud providers needed when on-demand. Second layer is authentication, which helps to protect the unauthorized user’s entry to the cloud. Third layer is confidentiality, which ensures that the data can be accessed by the privileged cloud users only. Last layer is integrity, which ensures that cloud data could not be modified by unauthorized cloud users. Authentication technique can be used to protect the data from outsiders attack. Confidentiality could be used to protect the data from outsiders as well as insiders attack. If the confidentiality of the data is ensured completely, then integrity will also be ensured. If the data in cloud storage can’t be accessed by the intruders then it cannot be modified or altered by intruders. Even though the authentication mechanism is broken by the attackers, the data in the cloud is still be secured when an efficient confidentiality mechanism is used.

This paper proposes an efficient cloud storage confidentiality technique by using encryption and obfuscation technique. Encryption is the process of converting the readable text into unreadable form using an algorithm and a key. Obfuscation is same like encryption. Obfuscation is a process which disguises illegal users by implementing a particular mathematical function or using programming techniques.
Normally, confidentiality is ensured by encryption technique, but for the cloud environment encryption alone is not enough for data protection. Encryption is integrated with obfuscation technique. Obfuscation technique alone is also not enough to adopt for complete confidentiality of data in cloud storage because the user can find values through reverse engineering or by using brute force technique, which may compromise cloud data security. This paper uses encryption and obfuscation techniques in an integrated manner to protect the data from the attackers (insiders and outsiders). In the proposed technique, users should encrypt and obfuscate the data whatever they want to send to the cloud storage. Encryption and obfuscation could be done from user’s side.

2. DATABASE MANAGEMENT IN THE CLOUD

Outsourcing of database management [4] is a necessary component of cloud computing. Due to the rapid advancements in network technology, the cost of transmitting a terabyte of data over long distances has decreased significantly in the past decade. In addition, the total cost of data management is five to ten times higher than the initial acquisition cost. This will lead the enterprises to outsource their data with cloud storage provider with minimum rate [5]. Database outsourcing model will enable the cloud users for better utilization of their data.

Despite the advantages offered by cloud-based DBMS, many people still have apprehensions about them. This is most likely due to the various security issues that have yet to be dealt with. Security becomes a serious problem with cloud DBMS when there are many Virtual Machines (which might be accessing databases via any number of applications) that might be able to access the database without being noticed or setting off any alerts. In this type of situation, a malicious person could potentially obtain pertinent data or cause serious harm to the integral structure of the database, putting the entire system in risk. This is the main problem with the cloud data storage.

Thus, an efficient security model needs to address this issue in the cloud data storage. According to this paper, even through the data is accessed by malicious persons it cannot be read or modified by them.

3. RELATED WORK

Ensuring confidentiality of user’s data in cloud storage is the main research problem around the cloud computing. Cloud storage providers store users critical data; it needs to be secured. Cloud computing has a recent success in information technology and will dominate the IT industries in the coming years. Cloud computing also faces the overwhelming challenges. To ensure the proper physical, logical and personnel security controls, especially in cloud data storage are more significant. Moreover, while moving such large volumes of data, the management of the data may not be fully trustworthy. This section describes the research works which are related to ensure the confidentiality of data in cloud storage.

Database as a service (DaaS) is highly appreciated in business community because it saves hardware cost, cost of the technical people required to manage the database and it also saves the license cost of the database. Moreover, it offers reliable services and people can access their data 24 x 7 from anywhere provided the internet connection is available. Despite of all these advantages enterprises are reluctant to adopt DaaS, because of two types of threats that are associated with it. Firstly, it can be attacked by the hacker and secondly the privacy of data can be compromised by the administrators, managing the cloud database environment. To address this issue, Atiq ur Rehman [6] proposed a model that encrypt and obfuscate data on client side before sending to the cloud database. In addition paper offered a mechanism to query over encrypted and obfuscated data on server side. Once the required data is filtered on server side, it is transferred on client side where the de-obfuscation and decryption is performed. Experiment results are also highlighted showing the enhancement in performance due to obfuscation factor. This paper considered the SaaS application. But this proposal is adapt only to PaaS model.

In [7] Dr. Nashaat el-Khameesy and Hossam Abdel Rahman proposed a security policy and procedures explicit to enhance the Data storage security in the cloud. They had a Control Access Data Storage (CADS) that included the necessary policies, processes and control activities for the delivery of each of the Data service offerings. The collective control Data Storage encompasses the users, processes, and technology needed to maintain an environment that supports the effectiveness of specific controls and the control frameworks. The security, correctness of data made in cloud storage, and availability of the data files being stored on the distributed cloud servers. It must be guaranteed by providing security policy and procedure for Data Storage, Defense in Depth for Data Storage in the cloud, Correctness Verification and Error Localization computing. All these recommendations are only theoretically proposed.

R. Anitha et al. proposed a method for providing protection to the data stored at the data server through metadata in [8]. This process provides protection using a cipher key which is created from the features of metadata. In this model, the time required for generating the cipher key is proportional to the number of attributes in the metadata as well the algorithms used for cipher key generation. Their plan enforced safety by providing two novel features; 1. Security is provided by their proposed design, where the encryption and decryption keys cannot be compromised without the involvement of data owner and the Metadata Data Server (MDS). 2. The cipher key generated using the modified feistel network holds good for the avalanche effect as each round of the feistel function depends on the previous round value. This approach is time consuming for generation of cipher key.

B. Raja Sekhar et al. [9] introduced the Ciphertext policy attribute-based encryption (CP-ABE) which is a promising cryptographic solution to ensure the data security and integrity in cloud storage. It allows data owners to define their own access policies over user characteristics and enforce the policies on the data to be distributed. It provides a way of defining access policies based on various characteristics of the requestor, background, or the data object. Especially, ciphertext-policy attribute based encryption (CP-ABE) enables an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the ciphertext, and enforce it on the contents. Thus, each user with a different set of attributes is allowed to decrypt several pieces of data as per the security policy.

Siani Pearson et al. described a privacy manager [10] for cloud computing, which reduces the risk to the cloud computing user of their private data being stolen or misused. As a first line of defense, the privacy manager uses a feature called obfuscation. The idea is that instead of being present unencrypted in the cloud, the user’s private data is sent to the cloud in an obfuscated form. 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 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. 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 personas, 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.

4. PROPOSED CONFIDENTIALLY TECHNIQUE

Cloud computing provides an efficient storage setting to store and retrieve the cloud users critical data. Ensuring data security is a vital role to cloud users as well as cloud providers. This paper uses the confidentiality parameter to address the data security problems. Figure 2 represents the cloud storage confidentiality protection system using encryption and obfuscation technique. All the data must be encrypted or obfuscated before it is sent to the cloud database. Based on the type of the data, encryption or obfuscation can be used. Once the data is applied by proposed confidentiality technique, then the data is submitted to the cloud storage. Encryption and obfuscation of cloud data is done in the user side. The key used for encryption algorithm is generated in the user environment.

Algorithm #1
1. start
2. T=plaintext
3. if (isdigit(T)) then
   obfuscation_digits(T)
4. else
   encryption_text(T)
5. end if
6. end

Algorithm #2
1. obfuscation_digits(T)
2. start
3. for i=1 to size of(T)
4. D(i)=pow(T(i),2) //find square value of plain text value
5. RD(i)=round(D(i)) // Round off the square value
6. loop
7. for RD(i)<32||RD(i)>126 //Find the printable ASCII value for RD by subtract
   RD(i)=RD(i)-256 //256 until its value comes in between 32 to 126
8. loop
9. count=count+1 //count the no. of subtraction happened; this count
10. loop //value will be the key for deobfuscation
11. Check the resultant value in the range of printable
12. ASCII value
13. Convert the value into ASCII code (C)
14. // C-Cipher Text
15. end

Generally, Confidentiality is ensured by encryption algorithm. For cloud data storage, Symmetric encryption is best choice, because symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data [11]. Along with the encryption algorithm [12], this paper also uses the obfuscation technique to improve the data confidentiality in cloud storage.

Algorithm #1 is used to find out the type of data (T) which is ready to be stored in the cloud storage. Based on the type of data, encryption or obfuscation is applied on the data before forwarding to the cloud. If the data (T) are digits, then obfuscation technique is applied, if the data are alphabets or alphanumeric or special symbols then encryption is applied on the data. This algorithm will call the corresponding algorithm based on the data type of (T).

Algorithm #2 is used for obfuscation. This algorithm is used for numeric data type. Obfuscation is a technique by applying through specific mathematical functions or by using programming techniques. Obfuscation doesn’t use any key to mask the user’s data. But deobfuscation is only happened with a key which is generated during the process of obfuscation. Several obfuscation techniques are available in the literature. This paper uses two mathematical function namely pow() and round() functions. The pow() function is used to convert T into its square value (D). The round() function is used to rounded up the value of D into its nearest whole value (RD). From the rounded value (RD), find the printable ASCII value by subtracting 256 from RD value until the RD value reaches the range between printable ASCII values (32-127). Finally the resultant value is converted into ASCII character value. The example result of obfuscation algorithm is shown in table 3.
Algorithm #3 is used for encryption. This algorithm is used for alphabets or alphanumeric or special symbols. This is a symmetric encryption algorithm. The algorithm uses substitution and transposition technique to convert the plain text into cipher text. ASCII codes of the plain text are used throughout the algorithm. It uses four keys for encryption, and same keys are used for decryption also. The given plain text characters are converted into ASCII values. A square matrix is formed based on the number of character in the plaintext. The square matrix is divided into three matrices called upper (UMAT), diagonal (DMAT) and lower (LMAT) matrix. Apply the encryption to the matrices UMAT, DMAT and UMAT individually by using the key K1, K2, K3 respectively. Form a square matrix with encrypted value. Now read the text by column by column, order of reading the column is based on the Key K3. Finally the ASCII code values are converted into character value, this value is cipher text.

Algorithm #3
1. encryption_text(T)
2. start
3. Convert (T) into ASCII code
4. N = count (T)  
   // N-no.of character in T
5. Based on the value of N, form a square matrix MAT
   [MXM] > N, M=M  
   // M-order of matrix
6. Apply T into the matrix from left to right
7. Divide the Matrix MAT into three matrices called
   UMAT, DMAT, LMAT
   //UMAT-Upper Matrix
   //DMAT-Diagonal Matrix
   //LMAT-Lower Matrix
8. Read the Text T by UMAT(U), DMAT(D) and LMAT(L)matrix
   //U, D, L- text of upper, diagonal and lower matrix
   // generate the random number for keys
9. for i=1 to 3
10.Ki=random_num_gen()
11. loop
12. Get three random integer number as KEYS K1, K2, K3
   for each matrix
13. Apply the key K1, K2, K3 for U, D, L
   //U-K1, D-K2, L-K3
14. Apply the resultant text (from step 10) into another
   matrixMAT1 [MXM]
15. K4_random_str_gen()  
   //Generate random string value as a key called K4
16. Order the matrix based on the key K4
17. Read the matrix by column using the order of key K4
18. Resultant text from step 14 is converted from the
   ASCII code into character(C)
19. end
//C-Cipher Text

Algorithm #4 is used for generation of random integer number. This algorithm generates a random value each time it invoked. Algorithm #3 invokes algorithm #4 for three times to get three random numbers as keys K1, K2 and K3.

Algorithm #4
1. int random_num_gen()
2. start  
   // generation of random using random() class
3. ran=new random().nextInt(100)

Algorithm #5 is used for generation of random string value. This algorithm generates a string and returns it to encryption algorithm. This string value is used as key K4.

Algorithm #5
1. String random_str_gen()
2. Start
3. for i=1 to 3
4. ran=new random().nextInt(126)+32  
   // generate the random number
5. ran_str_buff=(char)ran  
   //generate the number into equivalent char
6. loop
7. return the string buffer value by converting it into string
8. ran_str=ran_str_buff.toString
9. end

Proposed cryptography technique uses encryption and obfuscation for the different type of data. Integration of obfuscation technique with encryption technique has given more confidentiality than when they are used separately. Confidentiality of cloud data is ensured by using this technique. This can protect the data in cloud storage from insiders as well as outsiders attack.

For simple understanding of the proposed cryptographic technique, consider a sample transactional table as shown below Table 1, to be stored in the cloud storage. This Table 1 values are encrypted and obfuscated by the proposed cryptographic technique.

<table>
<thead>
<tr>
<th>Trans_Id</th>
<th>Cust_Id</th>
<th>Item_Name</th>
<th>Quantity</th>
<th>Total_P</th>
</tr>
</thead>
<tbody>
<tr>
<td>TId_9999</td>
<td>X987ren</td>
<td>Chocolate</td>
<td>50</td>
<td>15</td>
</tr>
<tr>
<td>TId_0012</td>
<td>G123aro</td>
<td>Medicine</td>
<td>12</td>
<td>60</td>
</tr>
<tr>
<td>TId_923</td>
<td>B301sus</td>
<td>Himalaya</td>
<td>17</td>
<td>1500</td>
</tr>
<tr>
<td>TId_2304</td>
<td>C100mon</td>
<td>Bovonto</td>
<td>3</td>
<td>145</td>
</tr>
<tr>
<td>TId_9087</td>
<td>B002lav</td>
<td>Laxmi</td>
<td>9</td>
<td>100</td>
</tr>
<tr>
<td>TId_0012</td>
<td>G123aro</td>
<td>Medicine</td>
<td>12</td>
<td>60</td>
</tr>
</tbody>
</table>

Proposed cryptography technique is implemented in JAVA running in windows 7 operating system. Table 1 represents the plain text values of sample transactional table of a shopping mall. Table 2 represents the encrypted values of the table 1 using algorithm #3 only. Table 3 represents the encrypted and obfuscated values of the table 1 using algorithm #2 and #3.

<table>
<thead>
<tr>
<th>Trans_Id</th>
<th>Cust_Id</th>
<th>Item_Name</th>
<th>Quantity</th>
<th>Total_P</th>
</tr>
</thead>
<tbody>
<tr>
<td>TId_9999</td>
<td>X987ren</td>
<td>Chocolate</td>
<td>50</td>
<td>15</td>
</tr>
<tr>
<td>TId_0012</td>
<td>G123aro</td>
<td>Medicine</td>
<td>12</td>
<td>60</td>
</tr>
<tr>
<td>TId_923</td>
<td>B301sus</td>
<td>Himalaya</td>
<td>17</td>
<td>1500</td>
</tr>
<tr>
<td>TId_2304</td>
<td>C100mon</td>
<td>Bovonto</td>
<td>3</td>
<td>145</td>
</tr>
<tr>
<td>TId_9087</td>
<td>B002lav</td>
<td>Laxmi</td>
<td>9</td>
<td>100</td>
</tr>
<tr>
<td>TId_0012</td>
<td>G123aro</td>
<td>Medicine</td>
<td>12</td>
<td>60</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trans_Id</th>
<th>Cust_Id</th>
<th>Item_Name</th>
<th>Quantity</th>
<th>Total_P</th>
</tr>
</thead>
<tbody>
<tr>
<td>TId_9999</td>
<td>X987ren</td>
<td>Chocolate</td>
<td>50</td>
<td>15</td>
</tr>
<tr>
<td>TId_0012</td>
<td>G123aro</td>
<td>Medicine</td>
<td>12</td>
<td>60</td>
</tr>
<tr>
<td>TId_923</td>
<td>B301sus</td>
<td>Himalaya</td>
<td>17</td>
<td>1500</td>
</tr>
<tr>
<td>TId_2304</td>
<td>C100mon</td>
<td>Bovonto</td>
<td>3</td>
<td>145</td>
</tr>
<tr>
<td>TId_9087</td>
<td>B002lav</td>
<td>Laxmi</td>
<td>9</td>
<td>100</td>
</tr>
<tr>
<td>TId_0012</td>
<td>G123aro</td>
<td>Medicine</td>
<td>12</td>
<td>60</td>
</tr>
</tbody>
</table>

Table 2 shows the encrypted values of all columns in Table 1. In this table encryption algorithm alone is applied for any
types of value. Encrypted values in Table 2 shows similar values for same plain text occurred in different places of Table 1.

Based on the proposed technique, encryption and obfuscation can be applied on the Table 1. Alphabets and alphanumeric types of data are encrypted, and numeric types of data are obfuscated. The Table 3 shows the cipher text value of Table 1 using encryption and obfuscation.

User’s data like the transactional Table 1 is submitted to the cloud storage in the form of encrypted and obfuscated shown in Table 3. This will increase the data security in the cloud storage.

Table 3. Transactional table with cipher text using encryption and obfuscation

| jzUdbjup | L1pvL|k\n | RymhGnwhy | Zz|dljx|\& | m|wb | |ru| |
|----------|------|-----|----------|-----|-----|-----|-----|-----|-----|
| k<\g3mL?: | J<\y6x<5> | U,\{k\x| | 2 | @ | |
| k<\g5mLBU | K< 3x96? | Qm|kp|dlum | ! | j | |
| k<\g6mL:| L<\z3r94v | K\{y|w|rw\} | ) | ! | |
| kDg3mLBC | K<\#3d93u> | Uy\%\{dr|d\ry | Q | 0 | |
| k<\g3mL9> | P\{5u;4j- | Vuz|gl|m|q | 2 | 0 | |
| k\g<\n|LEBE | a|Cz|hA<-|E | Lomron|x! | F | c | |

By the observation of the above three tables, it is evident that the integration of encryption and obfuscation will give more security to the data stored in the cloud. Table 2 shows only encrypted value, if the hackers find logic, they will apply it to the entire field in table to get the whole record. But in case of proposed technique same logic is not applicable for all the fields in the table. So hackers will not be able to get the actual values from table. This definitely increases the confidentiality of the data stored in the cloud.

5. CONCLUSION

Cloud computing is profitable computing services to an individual and enterprise customers. But due to some of security problem in it, people might be reluctant to use it. Once the issues are resolved, cloud computing will be the trillion dollars business in the computing world. The data storage on un-trusted cloud makes data security as a challenging problem. Data security in the cloud is ensured by the confidentiality of sensitive data. This paper proposed a new cryptographic technique which is applied to address this problem. Encrypted data are stored on storage servers while secret key(s) are retained by data owner; access to the user is granted by issuing the corresponding data decryption keys. Along with encryption, obfuscation technique is used to increase the confidentiality of data. Algorithms are proposed for encryption and obfuscation technique. The user data are encrypted or obfuscated before they are forwarded to the cloud storage. Encryption only or obfuscation only is not sufficient for cloud data security. Hence in this paper, a new confidentiality technique namely Obfuscrypt techniques, has been proposed and implemented. From the results obtained, it is observed that this technique could offer better security to data stored on a cloud than the existing techniques that are based on encryption, obfuscation alone.

6. REFERENCE


AROCRYPT: A CONFIDENTIALITY TECHNIQUE FOR SECURING ENTERPRISE’s DATA IN CLOUD

Dr. L. Arockiam 1, S. Monikandan 2

1 Associate Professor, Dept. of Computer Science, St. Joseph’s College (Autonomous)
Tiruchirappalli, Tamil Nadu, India.
larockiam@yahoo.co.in

2 Research Scholar, Manonmaniam Sundaranar University,
Tirunelveli, Tamil Nadu, India.
moni.tamil@gmail.com

Abstract— Cloud dominates the IT enterprises by way of its computing services. One of the services provided by the cloud is data storage. Cloud storage mainly supports Small and Medium scale Enterprises (SMEs) by reducing their capital investments and maintenance of storage servers. Most of the SMEs are outsourcing their data to cloud storage. Enterprises’ data that are forwarded to the cloud have to be kept in the public cloud storage. Safety and security are the top most issues in cloud storage. The confidentiality parameter provides data storage security. This paper proposes a security service algorithm named AROcrypt to ensure the security of data stored in cloud storage. It also describes Security as a Service (SEaaS) in the cloud environment. Simulation was conducted using a security analysis tool with existing techniques. The proposed technique provides better performance and good security when compared with existing 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 are Software-as-a-Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) [3]. The primary usage of cloud computing services is data 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’s attacks 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 are various 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 various existing techniques like DES, 3DES and Blowfish [9][10][11].

Cryptography [12] is a technique used for encryption and decryption. There are several cryptography techniques available for encryption and decryption. Cryptographic techniques are classified 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 as asymmetric 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 efficient for 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 propose and 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. Security is also provided as a service. In figure 1, CSP1 provides SEaaS and also provides other services. Here, CSP1 is used only for security service, and not for storing the data. Users could store their data with other CSPs who provide storage as a service.

Figure 1 – CSP with 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 describes AROcrypt 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.
III. RELATED WORK

This section describes some of the related works already done in the field of cloud security. Senyk et al. [14] considered a problem to build secured cloud data storage for public cloud. This paper describes an architecture that consists of four components namely a 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] proposed a 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 values of each character. Assign a key and apply it on the text using the formula: E = (p + k + i) % 256, where p denotes 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 requiring additional storage. Here, Author has not mentioned where the characters position details are maintained.

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

Manpreet K et al. [10] presented a Cipher Cloud framework. It helps users to keep their data confidential on public cloud. To achieve this, the framework uses a two-step encryption process, by which all the data sent from the client to cloud and cloud to client is retained completely 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 compares the 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 the cloud 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 achieving the 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 outsourced in encrypted form [19]. Figure 3 shows the working procedure of SEaaS security 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 CSP1 instructs the KGMaaS in CSP2 to provide keys to the user who chooses particular 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 communicated to the user, not through CSP1.
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 CSP3.

Fig. 3. SEaaS working procedure

Figure 3 shows the process of encryption, key generation and storage by CSP1, CSP2 and CSP3 respectively. CSPs are independent to others. CSP3 provides Storage as a Service (STaaS) to store customer data. CSP2 has the key providing system and key management system. It maintains log table for key management. CSP1 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 service processes 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 received from a CSP to the user.

Algorithm #1 shows the proposed AROcrypt security service algorithm in CSP1. 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 x 25. The square matrix is divided into three matrices called upper (UMAT), diagonal (DMAT) and lower (LMAT) matrix. Apply the encryption to the matrices UMAT, DMAT and LMAT individually by using the keys K1, K2, K3 respectively. Another square matrix is constructed with an encrypted value. Now the text is read column by column. Order of understanding the column is based on order of Key K4. Finally, the ASCII code values are converted into character 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 then divide the T into 625 character blocks and form matrix for each block.
5. matc=N/625
6. if matc>0
   for i=1 to matc
      Divide the T into 625 blocks, N=n1, n2, n3,...np  // n1, n2, n3 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
   // M-order of matrix
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 K1, K2, K3 for each matrix.
13. Apply the key K1, K2, K3 for U, D, L to get first encrypted data
    // [U-K1, D-K2, L-K3]
14. Arrange the encrypted text into another matrix MAT1 [MXM] based on number character in the key K4
    // Get random string value as a key K4
15. Read the matrix MAT1 column by column in order of key K4
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 CSP2. This algorithm generates a random value. CSP1 instructs CSP2 to generate three integers valued key for K1, K2 and K3 and one string key for K4. These four keys are forwarded to the cloud user directly by CSP2.

Algorithm #2: Random Number Generation

1. int random_num_gen()
2. start
   // generation of random using random() class
3. ran=new random().nextInt(100)
Algorithm #3 is used for the generation of random string value from CSP. This algorithm generates a string as key $K_4$ and sends it to cloud users along with keys $K_1$, $K_2$ and $K_3$.

**Algorithm #3: Random String Generation**

1. `String random_str_gen()`
2. `Start`
3. `for i=1 to 3`
4. `ran=new random().nextInt(126)+32` // generate the random number
5. `ran_str_buff=(char)ran` // convert the number into equivalent char
6. `end loop` // return the string buffer value by converting it into string
7. `ran_str=ran_str_buff.toString`
8. `return ran_str`
9. `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 configuration as Microsoft 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 1 represents the time taken for encrypting the data using proposed AROcrypt and existing techniques like DES, 3DES and Blowfish.
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.
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**

<table>
<thead>
<tr>
<th>S.No</th>
<th>Techniques</th>
<th>Security Level (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>DES</td>
<td>74</td>
</tr>
<tr>
<td>2.</td>
<td>3DES</td>
<td>82</td>
</tr>
<tr>
<td>3.</td>
<td>Blow fish</td>
<td>78</td>
</tr>
<tr>
<td>4.</td>
<td>AROcrypt</td>
<td>89</td>
</tr>
</tbody>
</table>

Fig. 6. Comparison of 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 confidentiality 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 untrusted 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

Appendix - ii

Deployment of Cloud Server in Amazon
(ii) Deployment of Cloud Server in Amazon

Amazon Cloud server with Window server 2008 OS is used for simulation. Steps for deploying an Amazon EC2 cloud server is as follows,


2. Sign in into Amazon Management Console.

3. Amazon Web Service (AWS) Management Console Home Page. It lists all cloud services provided by Amazon. Click EC2 to deploy an Amazon EC2 server.
4. Dashboard of EC2 is shown below. Click **Launch Instance** to launch a server.
5. Seven steps to launch a server. First step, select an Amazon Machine Image.

6. Choose a Microsoft Windows 2008 machine image from free tier. Select 32-bit or 64-bit OS.
7. Second step, choose an instance type, choose micro instance for free.
8. Third step, instance configuration screen is displayed.

9. Fourth step, for micro instance, Amazon provides 30 GB storage as free, if users want more, they could add storage in size field in the below screen.
10. Fifth step, tag an instance to other instance. If any.

11. Sixth step, configure the security policy.
12. Seventh step, review the instance details. Click **Launch** to create a key pair for launching new instance.

13. Create key pair for security of the EC2 server.
14. Give a key pair name as key_aromo and click **Download Key Pair** to download a *key_aromo.pem* public key file to the local users’ machine. Click **Launch Instance** to deploy the EC2 server.

15. Now instance is launching with prescribed configuration.
16. Screen shows instance launching status.

![Launch Status](image1.png)

17. Instance for EC2 server is launched and ready to use.

![Launch Instance](image2.png)
18. EC2 Dashboard shows the resources allocated for 1 running instance

An Amazon EC2 server is deployed in the cloud environment. This cloud server is connected to users’ machine to simulate the AROMO procedures. Users’ data after encryption or obfuscation are stored in this cloud server. Security levels for each SSA is measured by Hackman tool. This tool is installed in this cloud server to measure the security level.
Appendix - iii

Connect EC2 server to User’s Machine
(iii) Connect EC2 Server to Users’ Machine

EC2 server is connected to users’ machine to install the Hackman tool and simulate this tool to measure the security level. Steps to connect EC2 server to users’ local machine are as follows,

1. Click **Connect** to connect the EC2 server to the users’ local machine.

2. Get password to connect the EC2 server, click **Get Password**.
3. Select the public key file download early to the local machine.

4. Select the `key_aromo.pem` public key file from users’ machine.

5. To get the password, click **Decrypt Password**.
6. Details of Username and Password to connect the EC2 server is given to users. Windows cloud server are connected through Remote Desktop Connection (RDC). Click **Download Remote Desktop File** to download it to the users’ machine.

![Remote Desktop Connection](image1.png)

7. Double click icon to open the Remote Desktop Connection. It asks to connect server, Click **Connect**.

![Remote Desktop Connection](image2.png)

8. RDC connects the server and asks the username and password, submit the credential to open the EC2 server in the users’ machine.

![Remote Desktop Connection](image3.png)
9. EC2 server is opened in the Remote Desktop Connection window.
10. Full screen mode of the EC2 server desktop in users’ machines.

11. EC2 server has C drive with 30 GB hard disk. Two IP Addresses are allocated for a server, Public and Private. Public IP is changed for each login to server and Private IP is not changed.
Appendix - iv

Simulation of ABC Hackman Tool to Analysis the SSAs
(iv) Simulation of ABC Hackman Tool to Analysis the SSAs

Simulation is conducted to measure the security level of each SSA. Data processed by SSAs in users’ machine are stored in the cloud server. Hackman tool is installed in the EC2 server. Data are attacked by the Hackman using dictionary and brute force attack to find the security level. Simulation process is described in the following steps.

1. Hackman tool is installed in the EC2 server.
2. The BCC_HACK.exe is the hacking application installed in the C:\Temp URL in EC2 server.

![Image of BCC_HACK.exe]

3. Plaintexts are processed by a SSA in users’ machine. Processed data are stored in C:\Temp\decd.txt. The decd.txt shows encrypted data which are produced by AROcrypt SSA.

![Image of decd.txt]
4. Run the Hackman tool to analysis the security level of AROcrypt SSA by attack the encrypted data in *decd.txt*. During the simulation process Hackman ask the plaintext data of the encrypted data to measure the security level of the SSA. Plaintext is also stored in the C:\Temp folder.

5. Double click the *BCC_HACK.exe* to run the Hackman. It starts running.
6. Hackman is running now and it asks some details to attack and analysis the data.

7. Browse the plaintext file (plain.txt) to Source file, retrieved file by Hackman (dest.txt) to Destination file, encrypted file (decd.txt) to Decoded file, C:\Temp is working directory, BCC_HACK.exe is Security Analysis Tool and report file (report.txt) is Report file. Click Lunch.
8. Hackman starts analysis the each existing algorithms and proposed AROcrypt SSA. AROcrypt SSA is compared with DES, 3DES and Blowfish.

a. Analyzing DES

b. Analyzing 3DES
c. Analyzing Blowfish

![Blowfish Analysis Window]

```
Source File: C:\Temp\template.txt
Destination File: C:\Temp\encoded.txt
Decoded File: C:\Temp\decoded.txt
Working Directory: C:\Temp
Security Analysis Tool: C:\Temp/AROcRYPT_HACK.exe
Report File: C:\Temp\report.txt
```

![Launch Button]

**Launch**

**ANALYZE**

**GRAPH**

**EXIT**

---

**A 42**

---

d. Analyzing AROcrypt

![AROcrypt Analysis Window]

```
Source File: C:\Temp\template.txt
Destination File: C:\Temp\decoded.txt
Decoded File: C:\Temp\decoded.txt
Working Directory: C:\Temp
Security Analysis Tool: C:\Temp\AROcRYPT_HACK.exe
Report File: C:\Temp\report.txt
```

![Launch Button]

**Launch**

**ANALYZE**

**GRAPH**

**EXIT**
9. Hackman completes the analysis and produce a report with analysis details. Based on the report tables and graphs are generated.

The Hackman analyses the data for existing and proposed technique. In the same way, other two SSAs are analyzed with the corresponding existing technique to measure the security levels.
## Appendix - v

### Base64 Index Table
## (v) Base64 Index Table

<table>
<thead>
<tr>
<th>Value</th>
<th>Char</th>
<th>Value</th>
<th>Char</th>
<th>Value</th>
<th>Char</th>
<th>Value</th>
<th>Char</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>A</td>
<td>16</td>
<td>Q</td>
<td>32</td>
<td>g</td>
<td>48</td>
<td>w</td>
</tr>
<tr>
<td>1</td>
<td>B</td>
<td>17</td>
<td>R</td>
<td>33</td>
<td>h</td>
<td>49</td>
<td>x</td>
</tr>
<tr>
<td>2</td>
<td>C</td>
<td>18</td>
<td>S</td>
<td>34</td>
<td>i</td>
<td>50</td>
<td>y</td>
</tr>
<tr>
<td>3</td>
<td>D</td>
<td>19</td>
<td>T</td>
<td>35</td>
<td>j</td>
<td>51</td>
<td>z</td>
</tr>
<tr>
<td>4</td>
<td>E</td>
<td>20</td>
<td>U</td>
<td>36</td>
<td>k</td>
<td>52</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>F</td>
<td>21</td>
<td>V</td>
<td>37</td>
<td>l</td>
<td>53</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>G</td>
<td>22</td>
<td>W</td>
<td>38</td>
<td>m</td>
<td>54</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>H</td>
<td>23</td>
<td>X</td>
<td>39</td>
<td>n</td>
<td>55</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>I</td>
<td>24</td>
<td>Y</td>
<td>40</td>
<td>o</td>
<td>56</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>J</td>
<td>25</td>
<td>Z</td>
<td>41</td>
<td>p</td>
<td>57</td>
<td>5</td>
</tr>
<tr>
<td>10</td>
<td>K</td>
<td>26</td>
<td>a</td>
<td>42</td>
<td>q</td>
<td>58</td>
<td>6</td>
</tr>
<tr>
<td>11</td>
<td>L</td>
<td>27</td>
<td>b</td>
<td>43</td>
<td>r</td>
<td>59</td>
<td>7</td>
</tr>
<tr>
<td>12</td>
<td>M</td>
<td>28</td>
<td>c</td>
<td>44</td>
<td>s</td>
<td>60</td>
<td>8</td>
</tr>
<tr>
<td>13</td>
<td>N</td>
<td>29</td>
<td>d</td>
<td>45</td>
<td>t</td>
<td>61</td>
<td>9</td>
</tr>
<tr>
<td>14</td>
<td>O</td>
<td>30</td>
<td>e</td>
<td>46</td>
<td>u</td>
<td>62</td>
<td>+</td>
</tr>
<tr>
<td>15</td>
<td>P</td>
<td>31</td>
<td>f</td>
<td>47</td>
<td>v</td>
<td>63</td>
<td>/</td>
</tr>
</tbody>
</table>
Appendix - vi

Scopus Index of the Research Scholar’s Publications and Citations
(vi) Scopus Index of the Research Scholar’s Publications and Citations
Appendix - vii

Google Scholar’s Index of the Research Scholar’s Publications and Citations
(vii) Google Scholar’s Index of the Research Scholar’s Publications and Citations

<table>
<thead>
<tr>
<th>Title</th>
<th>Citations</th>
<th>Since 2015</th>
<th>Citations</th>
<th>Since 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIBM-CRU: An implementation of modified web cache replacement algorithm</td>
<td>11</td>
<td>2009</td>
<td>0</td>
<td>2013</td>
</tr>
<tr>
<td>Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm</td>
<td>7</td>
<td>2011</td>
<td>2</td>
<td>2012</td>
</tr>
<tr>
<td>Cloud computing: a survey</td>
<td>1</td>
<td>2014</td>
<td>0</td>
<td>2015</td>
</tr>
<tr>
<td>Optikrypt: A Novel Confidentiality Technique for Cloud Storage</td>
<td>2013</td>
<td></td>
<td>2014</td>
<td></td>
</tr>
<tr>
<td>Efficient Cloud Storage Confidentiality to Ensure Data Security</td>
<td>2014</td>
<td></td>
<td>2014</td>
<td></td>
</tr>
<tr>
<td>Cloud Service Tools: State of the Art</td>
<td>2013</td>
<td></td>
<td>2014</td>
<td></td>
</tr>
</tbody>
</table>
Appendix - viii

Academia.edu Index of the Research Scholar's Publications and Citations
(viii) Academia.edu Index of the Research Scholar’s Publications and Citations

Monikandan Shan
Department: Computer Science and Engineering, IIT Madras, India.

About

Papers

Add Section

Posts

CV

Recent Activity

Monikandan published a paper titled “Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm”.

Monikandan published a paper titled “Cloud Service Tools: State of the Art”.

Monikandan published a paper titled “SEMARI: An implementation of modified web cache replacement algorithm”.

Monikandan published a paper titled “Security Framework to Ensure the Confidentiality of Outsourced Data in Public Cloud Storage”.

Monikandan published a paper titled “Privacy in Cloud computing: A Survey”.

R
c

PAPERS

Efficient Cloud Storage Confidentiality to Ensure Data Security

Cloud computing: A Survey

Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm

Cloud Service Tools: State of the Art

SEMARI: An implementation of modified web cache replacement algorithm

Security Framework to Ensure the Confidentiality of Outsourced Data in Public Cloud Storage

Privacy in Cloud computing: A Survey

327

Total View

34

Followers

11 Following

Freelance Academics

Postdoctoral Researcher

Specialising in Computer Vision and Machine Learning

Master’s and Doctoral Scholarships in Public Policy

The EU Lisbon of Public Policy is dedicated to acquiring outstanding leadership students from around the world.

Master’s and Doctoral Scholarships in Political Science

Central European University

A47