An Integrated Secure Cloud Storage Architecture for Ensuring Integrity of Data using Hybrid Encryption Schemes in Cloud IoT Environment

Prof. Y. Sunil Raj, Dr. S. Albert Rabara & Mr. V. K. Sanjeevi

Assistant Professor, Department of Computer Science, St. Joseph's College (Autonomous), Trichy, India
Associate Professor, Department of Computer Science, St. Joseph's College (Autonomous), Trichy, India
Research Scholar, Department of Computer Science, St. Joseph's College (Autonomous), Trichy, India

ysrsjccs@gmail.com, a_rabara@yahoo.com, vksanvi@gmail.com

Abstract
Cloud computing revolutionize the way internet is used during the past few decades. As providing everything in an outsourced fashion, it provides infrastructures such as storage too. Though everything makes it easy for as to store and access data in a fastest and easy manner, their exist security risks if not handled become more dangerous. Strengthening of security in cloud storage is need of the hour, as it is the future technology which is changing the way business is done. This paper analysing the existing security mechanisms and algorithms, could present a novel architecture for enhancing the security of storage. In order to enhance the security, systematicuse of a hybrid algorithm along with a hashing technique is proposed. The validity of the mechanism have been analysed and ensured that if implemented will present better results to the cloud architecture.

Keywords: Cloud Storage, Data Integrity, Encryption, Hashing, DNA, MD5

I. Introduction

Cloud computing being a major technology which outsources almost every as services, is hiding the presence of chief corner stone called Internet. Without its presence, probably Cloud would be existing inside the womb of simpler networks waiting for the birth of Internet. The support of this great giantInfrastructure, Software, and Platform were distributed as service in low cost. Among these infrastructure would encapsulate things such as storage, networking, computation and virtualization.

In this IoT era, data is generated by most living and artificial objects. The data generated by the IoT is shared over the internet, and will be stored on cloud storage. This have become very essential because scaling the size of local storage will be more expensive. As a result most organizations have started using cloud storage for business related transactions. A number of research have been done and architectures have been devised. [Raj et. al., 2019]. Security issues can be resisted with a good architecture. Being a good architecture is alone not enough to secure data. It also requires other security mechanisms to protect the data. The work first analysis the issues that exists in the cloud that allows the data integrity to be affected.

1.1. Security Issues

As everything is available public, security of data becomes the major issue. Also every data is copied to a remote machine adds still more security risks. Therefore using proper security mechanism is very essential to keep the data safe and secure, preventing it from security attacks.

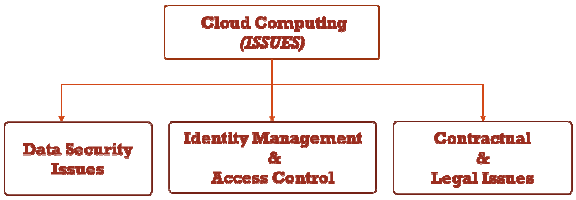

Fig. 1.1 Security Issues in Cloud Computing

The security attacks can be classified as storage based attacks, access control based attacks, identity attacks, contractual and legal issues. Among these analysing storage related attacks could enhance the security of storage, as it is where data stays for a long period of time. Major issues related to data storage are depicted in Fig 1.2.

Fig. 1.2. Data related Issues

1.1.1 Data in-transit

The communication among the entities with a secured communication channel like Transport Layer Security, may give rise to the following issues such as data lineage and data provenance.

Data Lineage: Data lineage is related to the origin of the data and where it moves over a time period. **[Bhadauria,**

et al., 2012], have proposed tracing the path of the data as data lineage. It helps in auditing. It is one of the challenging and tedious issues involved in tracing due to the non-linear nature of the cloud environment.

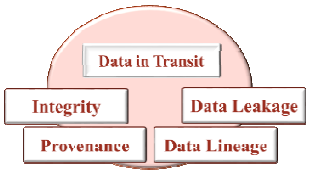

Fig. 1.3. Issues Related to Data in Transit

Data Leakage: Once the data is accessed by multi-tenant, the issue of data leakage arises.**[Sabahi, 2012]**, identified data leakage as one of the important security issues. **[Chen, et al., 2012]**, pointed out to the presence of a serious leakage of a user's private data, due to inherent security vulnerabilities in Google Docs. The danger of data leakage is substantial, requiring careful handling. Some of the challenges related to data leakage are, Instance Messaging, Email, Web Mail, Blogs / Wikis, Malicious Web Pages, File Transfer Protocol (FTP) and Universal Serial Bus(USB)/ Mass storage device.

1.1.2. Data- in-rest

[Vyas, et al., 2017], proposed an approach to secure storage of data in the cloud and performance integrity check on the stored data when accessing the data. Storing Encrypted file, hash file and meta-data in cloud improves the security of stored data in the cloud. **[Chatterjee, et al, 2017]** has presented review methods to ensure data security in the cloud, with the use of cryptographic measures to achieve privacy.

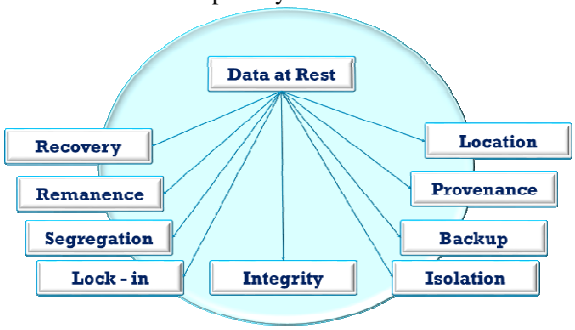

Fig. 1.4. Issues Related to Data in Rest

Data Recovery: The process of accessing data which is corrupted/damaged from the storage media is known as data recovery. The four phases of data recovery are depicted in Fig. 11. On deletion of a file, only the metadata is removed but the actual data remains on the disk. It can be recovered using file carving. Some commonly used Carving schemes are Bifragment gap carving, Smart Carving and Carving memory dumps. Common challenges to data recovery are OS failure, drive-level failure and deletion of file from a storage medium. These challenges have to be met.

Data Remanence/Sanitization/Removal: Data must be erased securely at the end of its life cycle. Overwriting is one of the traditional solutions for sanitizing data. According to **[Chen, et al., 2012]**, the physical characteristics enable restore/recovery of deleted data, leading to disclosure of sensitive data. With proper skills and equipment, it is possible to recover data from failed devices. The remanence of the data after deletion require attention.

Data Backup: Frequent updating of data results in data loss. Data backup in cloud storage or external server is required for handling loss of data. **[Bhargav, et al., 2015]** have specified a 3-2-1 rule, involving 3 copies of important files: 1-primary and 2- backups. They maintain the copies in 2 different storage media to defend against different types of attacks. Store 1 copy off-site. Maintenance of replication leads to security issues.

Data isolation: There should be a perfect separation between non-sensitive and sensitive data. Data should be isolated from unauthorized users through use of access control and encryption schemes. Fine-grained access control can be achieved through a user's identity, some of them are attribute-based, time- based etc. Isolation is a special kind of privacy. Lack of care in handling leads to VM to VM attack, there-by losing the confidentiality of the users.

Data segregation: Segregation of data refers to full separation between the cloud users in a virtualized environment. **[Negi, et al., 2015]**, have suggested that data segregation is an issue that is raised due to multi-tenancy. Cloud providers should use highly secured protocols and encryption algorithms to achieve data segregation. Data Segregation vulnerabilities arise due to data validation, insecure storage and SQL injection flaws. Meeting the specified uses in a multi-tenant environment, is of great help in mitigating the problem of data segregation challenge.

Data Lock-in: Data Lock-in is the main obstacle to achievement of portability and interoperability. **[Sax, et al., 2014]**, say that, in an industry insight, clearly outlined, the risk of cloud provider lock-in prevent the movement of data into, around and out of the cloud. The lock-in nature makes integration of data from different locations a difficult job. Consumers of the cloud should not get affected through this issue with a specific vendor.

Data Location: Storage as a service is highly dependent on the location of the data. Since the location of the data is not known to the users, users hesitate to store their sensitive data in the cloud. It is one of the common issues faced by organizations. The unknown location of data leads to questions of security, legal and requirements of regulatory compliance. This is one of the challenging issues due to untrusted cloud service providers.

1.1.3. Issues on data in-transit and at rest

Data Integrity: Integrity refers to data accessed or modified by authorized entities alone. Integrity checks can be performed with/ without third party audit. **[Kaur, et al., 2016]** on the other hand, proposed a data correctness scheme which involved a third party audit and ensured the safety of data. Regardless of data, both static and dynamic data should be protected from unauthorized observation, modification, or interference.

Data Provenance: Provenance includes the integrity of the data as well as their computational accuracy (integrity + computational accuracy = provenance). However, **[Asghar, et al., 2011]**, outlined that the description of how data is produced is provenance, therefore making it important for post-incident investigations. **[Martin, et al., 2012]**, presented a riskbased approach to provenance. Some of the challenges that arose from the data provenance included computational overhead, storage overhead, platform independence and application independence among others.

The cryptographic approaches could provide user-centred access control. This can be classified as, Public-Key Encryption - which does one-way encrypted transfer, Identity-Based Encryption – that encrypts the data based on identity, Attribute-Based Encryption – that enables control based on attributes, Functional Encryption - which requires private key holders to understand functions of plain text.

II. Review of Literature

[Sajay et al., 2019], have proposeda hybrid encryption technique, where homographic encryption and blowfish are the participants making the technique unique. The flexibility of homographic algorithm and security measures of blowfish algorithm combines together to make the storage more efficient.

[Jinan et al., 2019], have proposed a model for enhancing the security of data in cloud storage, while introducing a proxy re-encryption mechanism for the same. The mechanism stands unique as it could transform cipher text of IBE to PKE type text. The user can share private data in more secure manner. Other issues such as performance and dynamic data privacy protection is to be handled.

[Israa et al., 2019], have proposed an algorithm for enhancing the security by increasing the complexity in key generation. Authors also have suggested using double security by RSA algorithm could enhance the security of data. Thus saving the data from security threats.

[Changzhi et al., 2019], have introduced a compression and authentication algorithm that could maintain the security of data. The SVD is used to decompose the image considering them into three value matrix form. An authentication value is maintained for the cipher text data which improves the security of data storage.

[Irfan et al., 2018] have designedan architecture for distributed cloud storage with security framework to eliminate threats related to data at rest. The Secure Distributed Adaptive Bin Packing algorithm, uniquely allocates storage which enhances the security of the cloud storage. Also authors prescribes the algorithm to be performing better than first fit and best fit allocation schemes.

The study conducted by **[Sharmila, et al., 2018]**, on data masking technique have suggested the best algorithm for enhancing the security of storage on cloud. Major masking technique is categorized as static data masking and dynamic data masking. The techniques analysed was shuffling, substitution, random substitution, number, nulling and encryption.

[Shinde S, et al., 2018] have suggested an auditing technique using TPA for verifying the integrity of data. The proposel makes use of AES for verification of data and Secure Hashing Algorithm (SHA - 2) for generating verification metadata and message digest for checking integrity.

[Sreeja et al., 2017] have proposedDNA based cryptographic algorithm for securing data on cloud. Authors have used indexing and steganography along with binary coding rules. This biosecurity is largely secure than the conventional cryptographic algorithms.

[Thirupalu et al., 2018], discusses the symmetric and asymmetric algorithms for enhancing security in cloud, while introducing a new approach of public key cryptosystem. Enhancing the RSA algorithm authors have obtained the better result while improving the security concerns in cloud.

[Suganya et al., 2017] have proposed a cloud auditing technique that provides uninterrupted certificates to user and auditing the data using a new integrity checking protocol. Addressing the issues like modification of data in Multi-Cloud, they have proposed a continuous auditing method that verifies such process at block level and file level to ensure integrity. The cloud auditor is provided with the FAT for auditing, while blocks are generated at random based on the request.

[Weiwei et al., 2017] have proposed a secure proof of ownership scheme to support file rating. Here authors have used K-means algorithm along with random seed technique to achieve safe and efficient proof of work. This is most suitable of the cloud storage system that work under deduplication mechanism.

[Kajal. R. et al, 2017] have introduced a strategy, using steganography and splitting the storage in order to add security to the storage. The compression technique used could help reducing the space required to a greater extend. The process of security involved is locking folder, adding multimedia file, splitting the file, compress the file, encrypt the file and store. This enhances the security and while considering other factors

such as working with multimedia content become more tedious and time consuming with response time.

[Vijay et al., 2017]have introduced a role based encryption mechanism for securing the EAR. This also provide access to the storage based on the role in flexible manner. Authors have used BLOWFISH symmetric encryption algorithm with 160 bit key length along with ISAAC symmetric encryption algorithm.

The efficiency of security algorithms have been compared by **[Nasarul I. K. V, et al., 2017]**, to provide solution for the existing security threats in cloud. Authors have done the study on the known algorithms such as RSA, DES and AES. After the analysis they have suggested that homomorphic algorithms may best suit the cloud environment for enabling higher level of security.

[Swetha., 2017] have proposed an auditing technique in order to overcome the existing security threats. Here author have suggested continuous auditing technique along with the creation of signature for blocks using MD5 algorithm. Encryption of algorithm is done using Base64 algorithm.In order to verify the data integrity, author proposes, two step checking process they are block and file check.

[Saritha, et al., 2017] have compared various symmetric, asymmetric and hashing algorithms. The symmetric algorithms such as DES, 3DES, AES and Blowfish algorithms have been considered. Asymmetric algorithms such as RSA and Diffihufmen algorithms and MD5 hashing algorithm were included for the analysis. Analysis was done based on various parameters such as key size, security rate, throughput, block size, scalability, speed and encryption/decryption. It was inferred that blowfish algorithm was efficient among the algorithms selected for the study.

[Ashalatha, et al., 2016] have designed a mechanism for enhancing data audibility. Authors have also discussed about various security algorithms used for safeguarding the public cloud. The auditing process is done in various levels such as public audit, dynamic audit also called as integrity proof and batch audit. Though this mechanism help retaining the data to a greater extent, it would obviously during the time required for handling the whole process.

[Mohamed. I, et al., 2016] have addressed the security threats in cloud storage. They have proposed a storage authentication and data encryption schemes for protecting the data storage. Here AES cryptographic algorithm is used for encryption and the validity of the user is verified to deny unauthorized access. Authors have focused on enhancing the privacy of data, avoid data loss and enhance availability of data. Thus enhancing the security of remote storage.

A review on symmetric and asymmetric algorithms have been done by **[Akashdeep. B, et al., 2016]** with emphasis on symmetric algorithms. Here authors have suggested the algorithm that best suit data and link encryption. As the parameters of various algorithms have been analysed it was concluded that AES algorithm is best for key encryption and MD5 would perform better in encoding the data.

Ali et al., [2015] have introduced an architecture for inter-cloud data transfer based on cryptographic algorithm. The technique proposed uses a two phase encryption/ decryption for file upload and download, i.e., encrypting the data using AES algorithm and then encrypting the key using Elgamal algorithm.

Xiaoyan et al., [2015] have proposed an architecture to ensure the integrity of the query results. This uses **C**ounting **B**loom **F**ilters to generate proof for users and also proposes a hybrid model for guarantee the search efficiency.

[Raj et. al., 2020] after analysing various techniques have concluded that hybrid approaches would provide better security to the data on the cloud. Therefore devising hybrid algorithm is a better solution for keeping the security of data at rest.

Table 1. Analysis of the Existing Algorithms

	Technique	Model	Efficiency	Storage
Xiaoyan et al., [2015]	Counting Bloom Filters	Hybrid	Search	No
Ali et al., [2015]	AES & Elgamal	Hybrid	Upload & Download	No
Mohamed. I, et al., 2016	AES	Hybrid	Storage	Yes
Ashalatha, et al., 2016	Auditing	New	Storage	Yes
Sreeja et al., 2018	DNA, Steganography	DNA	Data	No

Table 1, presents an analysis of the existing algorithms based on various parameters. Here the integrity concerns to be strengthened with respect to the storage that is to protect the data at rest. This is to be considered in the further sections by devising a security algorithm based on DNA cryptosystem.

III. Proposed Architecture

As security of cloud storage have to be strengthened, the study have been made on this context and is presented in the above section. It was observed lot of algorithms have been introduce and few mechanisms have been drawn. But an end to end security architecture found is very few in number, therefore a novel architecture is proposed as in the figure 3.1.

3.1. SecCS Architecture

Modelling of an architecture is required for getting into a new proposal for improving the existing communication and storage mechanisms. Here the architecture is intended to provide end to end security, so as to prevent the data in transit. The main objective is to strengthening the security of data at rest. As data have no intelligence,

it is necessary for us to find a proper security mechanism to help it keep the integrity.

The figure show the **SecCS** architecture who is enhancing the security of data in two major aspects as it was discussed earlier in this section. The model is composed of four components, where IoT devices layer, IoT user layer, Cloud Storage Layer and Cloud Processing layer.

a) IoT Device Layer

This layer is composed of the smart devices that will be used to provide services to the user. This totally application specific. The sensors and actuators present can be used in applications like motion, proximity and other such in transport applications. Sensors such as heart beat sensor, blood pressure sensor can be used in health applications. Thus devices working in the field will be employed in this layer.

The data generated in large amount will be in this layer. The data generated will be transferred using **CoAP**protocol and will be transmitted to the WWW using an **EDGE**who actually will translating the **CoAP** protocol into **HTTP** protocol specific.

b) IoT User

This is the layer where smart devices are used by various type of users in different ways. Here the devices are used to monitor or to identify the status of the devices in the field. The devices at this end is also let to function in **CoAP** as it is a light weight protocol. The data received might be earlier subject to a thorough statistical analysis. Here the use of device is to handle the real life task in most controlled way.

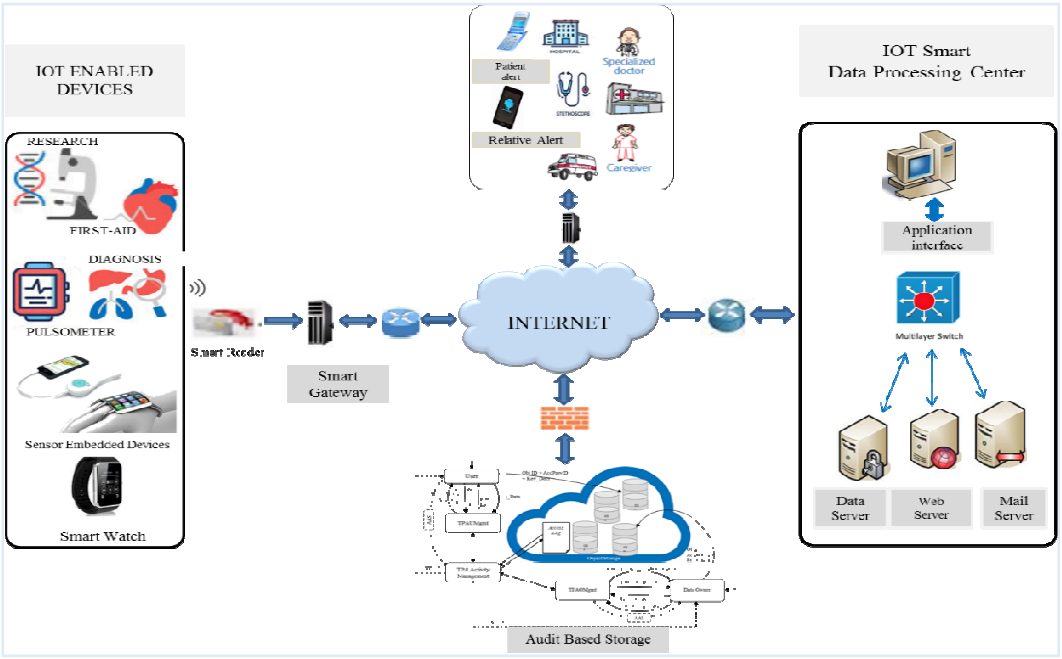

Fig. 3.1. An Integrated Secured Architecture to Ensure Integrity in Data Storage using Hybrid Encryption Scheme in IoT Cloud Environment

This layer receives the data form **EDGE**whoconvert the **HTTP** protocol content in to **CoAP**, smart device understandable contents.

c) Cloud Storage

The largely used storage component requires, central Third Part Auditors for managing the $\mathbf{TPA_{user}}$ maintaining the Data Dictionary and Users Privileges at service user end. $\mathbf{TPA_{user}}$ would continually monitor the Access.

The $\mathbf{TPA_{owner}}$ control the data owners regardless of the process they do with storage. Here both Service user and provider is assigned audit mechanisms, thus verifying TPAs activities.

The **DNA** algorithm is used to encrypt the data at the first level and then **BLOWFISH** algorithm is used for encrypting the data at second level. After this the data will be let to be stored in the allocated storage along with the generated hash using **MD5**.

d) Cloud Processing

Processing an important component for keeping the intelligence of the entire system. The processing layer of the proposed architecture is

assigned with duties like analytics, user and data management processes.

3.2. SAEICSAlgorithm

The end to end security architecture enhances the security of data in transit, so that MIMA is avoided to a larger extent. In order to improve the security of data at rest it is essential to have stronger security mechanism so as to protect the data. The proposed algorithm is a hybrid algorithm with the presence of DNA algorithm working at the first level encrypting the data and then at the second level the asymmetric Diffie-Hellman algorithm plays its role further encrypting the data.

3.2.1 Hybrid Algorithm in Action

Encryption Using DNA Algorithm

The hybrid approach is more efficient as it undergoes two levels of encryption. As per the proposed architecture the data received is encrypted using DNA algorithm. The DNA algorithm takes binary values and work on them generating substitution process. The final encrypted if converted to a normal string world display a different format. The encryption algorithm drawn for enhancing the security to a greater extent is described below.

```
Encryption (planetextp)
Begin
        acypt[i]=ascii(p);
        bcypt[i]=bin(acypt[i]);
        while(bcypt[i])
                while(length(bcypt[i])!=0)
                        pacypt[i]=substr(bcypt[i],2)
                end
        end
        while(pacypt[i])
                switch(pacypt[i])
                        case 00:
                                dntxt[i]=A;
                                break;
                        case 01:
                                dntxt[i]=T;
                                break;
                        case 10:
                                dntxt[i]=G;
                                break;
                        case 11:
                                dntxt[i]=C;
                                break;
        end
        nuctbl=construct(table(rand(0,9)));
        while(dntxt[i])
        if(dntxt[i] &&dntxt[++i] &&dntxt[++i] &&
dntxt[++i])
                        cypt[j]=nuctbl(dntxt);
        end if
        end
        pk=k;
        py=k;
        foreach(cypt)
                sectxt=blowfish(cypt, pk)
        end
        write (sectxt);
End
```

The duty of the broker is not only to allocate storage, but to provide a new form to the text that is received so as to protect the data. The encryption is subjected to start by receiving the text from the internet, receiving at the receiving end. The data received is subjected to the calculation of ASCII and the data will be replaced with its equivalent ASCII. Now after the ASCII is grouped properly, binary equivalent will be calculated. The ASCII will be replaced with binary equivalent. After this the binary digits are grouped into twos, so as to replace them with DNA codes. The grouped codes will be replaced with A or T or G or C respectively, by checking the pairs. As each pair is having its own code, it is essential to verify the digits while this replacement is done. As this iteration is completed the data received will be converted into a totally different form, which may resemble a bimolecular data.

The DNA codes are further subjected to a set of substitution. For this a nucleoid table is constructed, whose initial value is generated using a random number. The subsequent numbers will follow the random number by gradually increasing with 1. This makes this algorithm unique, which makes the identification of values are little more risky. The generated code is substituted for the DNA found in the order. For the set of every four nucleotides the equivalent code is substituted. The resultant cypher text will be totally different digit, this increases the safety of data.

As hybridisation is customary and also since it suits enhancing the security, cypher text thus obtained is collected for further encryption. The text is again passed through BLOWFISH algorithm. This is believed to enhance the visibility of data.

After subjecting the data into two phase encryption the data will be surrendered back to the broker. The broker will decide now how to break the data and where to store each and every block. Each and every block will be uniquely identified using signatures, generated by MD5.

Decryption Using DNA Algorithm

The encrypted text can be decrypted by substitution of the bits back to the previous pattern. The decryption algorithm is as follows:

```
        Decryption (b, r)
        Begin
                Cypt=BLOWFISH(b);
```

```
            Cypt=nucliotoid(cypt, r);
            necypt[i]=cypt[i];
            bcypt[j]=bin(necypt[i]);
            acypt[i]=ascii(bcypt[i]);
            t=acypt[i];
        End
```

The process of decryption is an inverse process of encryption. Though it is proved, it is better to display the decryption mechanism too. The BLOWFISH is let to handle the uncovering of the outer cover which is the first level of decryption to receive the actual data. Now as the integers are received as output, the operation of finding out the relevant DNA sequence is done. Once the sequence is found the integer will be replaced with the sequence identified. Now the output received in this iteration is converting every integer into the sequence of DNA codes.

Now each and every set of codes will be treated as individual characters, and the binary equivalent of this character is replaced after analysing. After the binary value of every character is found, the ascii equivalent of each and every set of binary value will be calculated. Every set of binary value will be replaced with its associated ascii code. Now it is the final task of finding out the actual text that was stored by the data owner.

IV. Results and Discussion

The **SAEICS**architecture have beensimulated and the results have been analysed. The data is presented as it is and also the graphical presentation explain the efficiency of the propose **SAEICS**algorithm.

4.1 Response Time

The efficiency of any algorithm in real application have to measure in the terms of its response time. As the response time of the proposed hybrid algorithm is found to be fair. Since the sole concentration of the work is to enhance the security, increasing the response time is not under the concern. However, the response time of the algorithm in the simulated environment is recorded as follows:

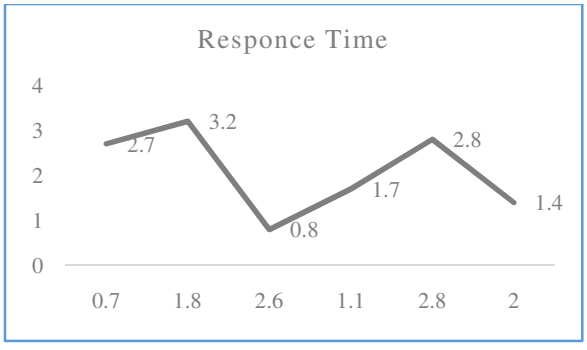

Fig 4.2. Response time of the Proposed Algorithm

The figure 4.2, depicts the response time of the algorithm, while the devices involved is 100. The results are noted in micro seconds, and are depicted in the figure.

4.3. Data before attack

The figure 4.3 shows the data on the storage. This represent the integrity of data on storage as the intruders where not simulated and security algorithm is not employed. The pictorial representation of data simulated are as follows:

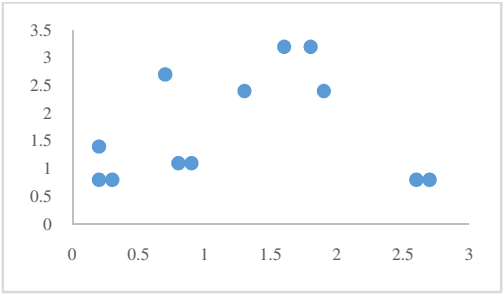

Fig. 4.3. Level of integrity

As the devices sampled randomly for simulation is 100. Among this around, 3% of the data is found to be not available for the user as it was affected due to system failure and other such issues.

44. Data after attack

The figure 4.4 shows the data on the storage after attack. This shows the level of attack before the algorithm is not implemented. The pictorial representation of data simulated are as follows:

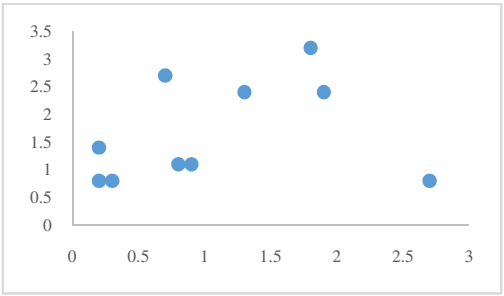

Fig. 4.4. Simulation of Attack – level of data integrity

As the devices sampled randomly for simulation is 100. Among this around, 94% of the cloud storage is not affected during the attack. As few have be modified due to the system failure and other physical disasters. Also the remaining being affected due to the absence of a strong security techniques.

4.5. Data stored using SAEICS technique

The figure 4.5 shows the data on the storage after attack, while there is a guard to protect it. This shows the level of integrity of data after the algorithm is implemented in an malicious environment. The pictorial representation of data simulated are as follows:

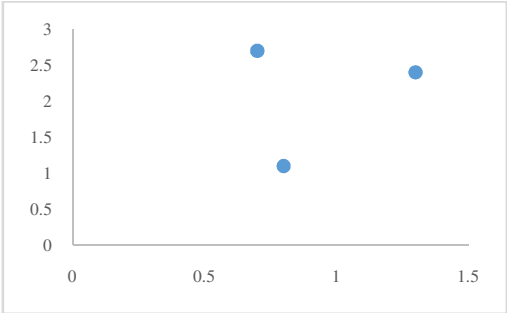

Fig. 4.5. Level of Integrity Monitored

As the devices sampled randomly for simulation is 100. Among this around, 3% of the cloud storage is affected during the attack. As few have be modified due to the system failure and other physical disasters which have to be handled in further studies.

4.6. Comparison

The objective of this section is to pictures the comparison of the proposed algorithm with the existing algorithms that are considered for studies.

Table 2. Comparison of the Technique

	Technique	Type	Handled
Mohamed. I, et al., 2016	AES	Hybrid	Storage
Ashalatha, et al., 2016	Auditing	New	Storage
Sreeja et al., 2018	Steganography	DNA	Data
Proposed Algorithm	DNA, Blowfish, MD5	Hybrid	Storage

The table 2, shows the need of the proposed technique for securing the data, by maintaining its integrity. The existing algorithms used by **[Sreeja et al., 2018],** requires hard computations for processing images. Therefore the proposed algorithm adding multiple level of encryption could require less amount of computation. As it was concluded by **[Raj et. al., 2020]** that Hybrid approach is best suited for public cloud environment. The proposed work could perform better than the existing algorithm, by decreasing the computation time largely.

V. Conclusion

Analysing the existing security mechanisms the work presents a novel architecture for enhancing the security of storage. To enhance the security SAEICSa hybrid encryption algorithm is introduced. This does encryption in two levels which strengthens the security of data at rest. The trace of the actual could be only recovered only after the two levels of decryption in the reverse order. The validity of the mechanism is ensured using simulation. The SAEICS is found performing better by presenting a higher level of integrity to the data. The disk encryption technique could enhance the security of data to a greater extent.

Reference

1. **[Raj et. al., 2020]** Mr. Sunil Raj Y, Dr. Albert Rabara S, Mrs. Helen Parimala E, "Enhanced TPABased Data Integrity Mechanism for Object Storage Architecture on Integrated IoT Cloud Smart Environment", Journal of Shanghai Jiaotong University, Vol. 16 (10), 2020, pp.153-161.
2. **[Raj et. al., 2020]** Sunil Raj Y, Lucase L, Helen Parimala E, "DNA Based Hybrid Approach for Data Integrity on Integrated Cloud Based Smart Environment: An Analysis", International Journal of Scientific Development and Research (IJSDR), 2020, pp. 194 – 205.
3. **[Raj et. al., 2019]**Sunil Raj Y, Albert Rabara S., "An Integrated Architecture for IoT Based Data Storage in Secure Smart MonitoringEnvironment", International Journal of Scientific & Technology Research, Vol 8(10), 2019, pp. 2213 – 2216.
4. **[Sajay et al., 2019]**Sajay, Suvanam Babu, Yeliepeddi, "Enhancing the security of cloud data using hybrid encryption algorithm", Journal of Ambient Intelligence and Humanized Computing, Springer, 2019, DOI: 10.1007/s12652-019-01403-1.
5. **[Israa et al., 2019]** Israa Al Barazanchi, Shihab Shawkat, Moayed Hameed, Khalid Saeed, "Modified RSA-based algorithm: a double secure approach", TELKOMNIKA, 2019, pp. 2818 – 2825.
6. **[Jinan et al., 2019]**Jinan Shen, Xuejian Deng, Zhenwu Xu, "Multi-security-level cloud storage system based on improved proxy re-encryption", EURASIP Journal on Wireless Communications and Networking, Springer, 2019, pp. 1-12.
7. **[Changzhi et al., 2019]** Changzi Yu, Hengjian Li, Xiyu Wang, "SVD-based image compression, encryption and identity authentication algorithm on cloud", IET Image Processing, The Institute of Engineering and Technology, 2019, pp. 2224 – 2232.
8. **[Irfan et al., 2018]**Irfan Mohiuddin, Ahmad Almogren, Mohammed Qurishi, Mohhammad Mehedi, Iehab Rassan, Giancarlo Fortino, "Secure Distributed Adaptive Bin packing Algorithm for Cloud Storage", Future Generation Computer Systems, 2018, DOI: 10.1016/j.future.2018.08.013.
9. **[Sharmila, et al., 2018]**Sharmila, Borgia Anne, Sreeja, "A Comprehensive Study of Data Masking Techniques on Cloud", International Journal of Pure and Applied Mathematics, Vol 119, 2018, pp. 3719 – 3727.
10. **[Shinde S, et al., 2018]**Soumya Shinde, Ramya V. Shinde, Priyanka Kamadhenu, "A Novel Data Auditing Approach to Achieve Data Privacy and Data Integrity in Cloud Computing", International Conference on New Horizons in Science Engineering Technology (NHSET-2018), IJSRCSEIT, 2018.
11. **[Sreeja et al., 2018]** Sreeja C. S, Misbahuddin M, "DNA Cryptography for Secure Data Storage in Cloud", International Journal of Network Security, Vol.20 (3), 2018, pp. 447 – 454.
12. **[Thirupalu et al., 2018]** Thirupaula, Spandhana, Kesavulu Reddy, "Security Analysis of Cryptographic Algorithms in Cloud Computing", International Journal of Engineering Research & Technology, Vol 7 (10), 2018, pp. 208 – 212.
13. **[Kajal. R. et al, 2017]**Kajal Rani, Raj Kumar, "Enhance Data Storage Security in Cloud Environment using Encryption, Compression and Splitting Technique", International Conference on Telecommunication and Networks, 2017.
14. **[Saritha, et al., 2017]**Kumari Sarita, Jawahar Thakur., "Data Centric Security Algorithms In Cloud Computing - A Review", International Journal for Research in Applied Science & Engineering Technology (IJRASET), 2017.
15. **[Suganya et al., 2017]**Sugnaya, Durai Raj, "Improving Cloud Security by Enhancing Remote Data Integrity Checking Algorithm", International Conference on Innovations in Power and Advanced Computing Technologies, IEEE, 2017, pp. 1 – 6.

16. **[Swetha., 2017]**Swetha M., "Creating Secure Cloud By Continuous Auditing Using DBM Algorithm",International Journal of Computer Science & Engineering Technology, 2017.
17. **[Vijay et al., 2017]** Lan Zhou, Vijay Varadharajan, Kanchi Gopinath, "A Secure Role-Based Cloud Storage System For Encrypted Patient-Centric Health Records", The British Computer Society,The Computer Journal, 2016.
18. **[Weiwei et al., 2017]**Weiwei Zhong, Zhusong Liu, "Efficient proof of ownership for cloudstorage systems",AIP Conference Proceedings, DOI: 10.1063/1.4992867, 2017.
19. **[Nasarul I. K. V, et al., 2017]**Nasarul Islam.K.V, Mohamed Riyas.K.V, "Analysis of Various Encryption Algorithms in Cloud Computing", International Journal of Computer Science and Mobile Computing, 2017.
20. **[Vyas, et al., 2017]** Vyas J. Prashant Modi, "Providing Confidentiality And Integrity On Data Stored In Cloud Storage By Hash And Meta-Data Approach", Int J Adv Res Eng, Sci. Technol. 2017.
21. **[Chatterjee, et al, 2017]** Chatterjee R, Roy S. "Cryptography in cloud computing: a basic approach to ensure security in cloud", IJESC, 2017.
22. **[Akashdeep. B, et al., 2016]** Akashdeep Bhardwaja, GVB Subrahmanyam, Vinay Avasthi, Hanumat Sastry, "Security Algorithms for Cloud Computing", International Conference on Computational Modeling and Security (CMS 2016), Science Direct, 2016.
23. **[Ashalatha, et al., 2016]**Ashalatha R, Jayashree Agarkhed, Siddarama Patil, "Data Storage Security Algorithms for Multi Cloud Environment", International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB 16),2016.
24. **[Kaur, et al., 2016]** Kaur S, Khurmi DS, "A Review on Security Issues in Cloud Computing", Int J Comput Sci Technol, 2016.
25. **[Mohamed. I, et al., 2016]**Mohamed Ismail, Badamasi Yusuf, "Ensuring Data Storage Security in Cloud Computing With Advanced Encryption Standard (AES) and Authentication Scheme (AS)", International Journal of Information System and Engineering, 2016.
26. **Ali et a., [2015]**, [20] Ali Azougaghe, Zaid Kartit An efficient algorithm for data security in cloud storage, IEEE, 2015.
27. **Xiaoyan et., al, [2015]**, Xiaoyan Zhu, Ripei Hao, Shunrong Jiang, Haotian Chi, Hongning Li,Verification of Boolean Queries over Outsourced Encrypted Data Based on Counting Bloom Filter, IEEE, 2015.
28. **[Bhargav, et al., 2015]** Bhargav Vora S, Anandache JG. Data Backup on: cloud computing Techniques in digital libraries perspective. J Global Res Comput Sci May 2015.
29. **[Negi, et al., 2015]** Negi T, Chaudhary S, Rautela S. Data security in cloud computing. Int J Adv Res Comput Sci Software Eng May 2015.
30. **[Sax, et al., 2014]** Sax R, Reeher J. How to avoid lock-in and ensure data portability in the cloud, Feb 13, 2014.
31. **[Bhadauria, et al., 2012]** Bhadauria R, Sanyal S. Survey on security issues in Cloud Computing and Associated Mitigation Techniques. Int J Comput Appl (0975-888) June 2012;47(18).
32. **[Martin, et al., 2012]** Martin A, Lyle J, Namilkuo C. Provenance as a security control, 2012
33. **[Sabahi, 2012]** Sabahi F., "Secure virtualization for cloud environment using hypervisor-based technology", Int J Mach Learn Comput, 2012.
34. **[Chen, et al., 2012]** Chen D, Zhao H. Data security and privacy protection issues in cloud computing, International conference on computer science and electronics engineering 2012.
35. **[Asghar, et al., 2011]** Asghar MR, Ion M, Russello G. Bruno Crispo2. Securing data provenance in the cloud, conference paper, 2011.