IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cloud Based EHR System for Secure Medical Data and Privacy Protection in Cloud Environment

[1]Ms. Vaishali Vijay Wagh, [2] Prof. Kishor N. Shedge

[1]PG Scholar, [2]Assitant Professor,

[1,2]Department of Computer Engineering,

[1,2] SVIT, Nashik, India

Abstract: Today, health data stored in the cloud is considered a highly confidential record, which must be hidden to prevent unauthorized access to protect patient information. Therefore, security issues related to moving medical data to the cloud have attracted the attention of researchers and scientists. A hybrid of data encryption models used to store diagnostic data in medical images. The proposed hybrid encryption scheme is based on the integration of Blowfish and encryption algorithms. our proposed framework applies a set of security constraints and access control that guarantee privacy and protection of medical information. We believe that the proposed framework paves the way for a new generation of lower cost, more efficient healthcare systems.

Index Terms **- EHR, Cloud computing, security, privacy, encryption. Blow Fish Algorithm, MD5.**

I. INTRODUCTION

Information security has become a major concern today. In today's trading world, no matter how data exists, whether it's basic conversation messages, complex medical information, or simple email messages, they must be exchanged data. Medical and personal data are regarded as a serious problem, which has caused great concern in the modern world. Therefore, the need for more reliable protection of online status is very important. Required to gain user trust. To ensure the security of online management and exchange, encryption technology is valued because it distributes unthought-out customer data to a more secure virtual world. Cryptographic calculations are symmetrical and asymmetrical. Symmetrical calculations, when contrasted and unbalanced, are incredibly fast and secure due to its solid key size. The proposed application uses a large number of hashes to ensure consistency. Use Blowfish symmetric key algorithm to encrypt information.

CP can perform most of these tasks to protect the data of its customers. In fact, the CP can share data and store each part on a different computer. You can encrypt data and add redundancy to avoid errors, etc. These measures can maintain customer trust and can be incorporated into service level agreements (SLAs). In some applications, including medical history For example, healthcare providers are responsible for maintaining the confidentiality of patient data. Although electricity can reduce the workload required to store a large amount of knowledge through the use of cloud storage, it is not enough to rely solely on the security measures of CP.

Therefore, this proposes method that can supplement any security measures taken by the CP. This can also be achieved if the CP does not protect the data in encrypted form. The proposed method does not require redundancy or increase storage costs, but can be easily implemented in combination with redundant methods. The main task of this method is to download the overhead associated with storing large amounts of customer data on the CP allows customers to be responsible for the security and privacy of their data, thereby providing an additional layer of data protection for critical applications such as medical records.

Service model Cloud computing has 4 unique service models:

1.1 **Software as a Service (SaaS):** A model in which an application is hosted as a service to customers who access it via the Internet. How to keep the infrastructure running. In the SaaS model, customers or consumers run applications on the provided cloud infrastructure Store software and organization's various applications on demand. Through the browser and application interface. In this model, customers no longer manipulate cloud infrastructure, networks or servers, storage or operating systems. Even Microsoft, Google and Zoho also provide SaaS.

1.2 **Platform as a Service (PaaS):** This model provides a foundation for rapid application development and deployment. PaaS refers to a cloud platform that provides a runtime environment for developing, testing, and managing applications. The solution provides a pay-as-you-go model. price. Examples of PaaS services are Heroku and Google's application engines.

1.3 **Infrastructure as a Service (IaaS):** IaaS provides users with an automated and scalable environment. IaaS is a cloud service that provides the underlying computing infrastructure: servers, storage, and network resources. In other words, IaaS is a virtual data center. In the pay-as-you-go model. Examples of IaaS provided by Elastic Compute Cloud or EC2.

1.4 **Everything as a Service (XaaS):** Provides a wide range of services, from personal services to key resources on the Internet. Examples: Hardware as a Service (HaaS), Communication as a Service (CaaS), Security as a Service (SECaaS) Health as a Service (HaaS) Transport as a Service.

Therefore, the most important results of this work are:

- A cloud-based health system is proposed, in which the confidentiality of user physiological data and the efficiency of data transmission are our main concerns. We use blowfish algorithm to protect data that is transmitted to the cloud.
- For data exchange in cloud packages, we use user affinity and reputation to build a trust model. Based on the confidence of the measured user, the system determines whether data exchange is taking place. Different types of clouds, and use encryption mechanisms to protect them accordingly.
- We provide cloud-based collaborative framework to protect users entire healthcare system from malicious attacks and atteker.

II. RELATED WORK

Our work is closely related to cloud-based data protection frameworks. We briefly summarized the work in these areas.

A modified form of the Blowfish encryption algorithm, which was developed to support the prompt method of 128-bit input, which in turn will lead to faster execution time of encryption functions executed in randomly defined rounds [1]. It's complicated, and the changes made show an overall performance improvement, designed to increase algorithm capacity and strength, while increasing its support for 128-bit input block sizes.

Archana Bharadwaj [2] contains human electrocardiogram reports, which are analyzed before the user must confirm the correct transaction ID and fingerprint, and then checked against the database. In this case, the level of two-factor authentication is increased. Both text files and image files can be encrypted and decrypted at the same time. This does not apply to large files, and using a single letter replacement algorithm puts you at risk.

Mohd Anuar Mat Isa [3] warned against accessing the same computing resources, because a fixed execution time can prevent synchronization attacks and reduce computing costs. In large-scale experiments, the key finding is that efficiency is an issue.
Aghili, H [4] within the paper proposes a way to confirm additional economical security victimization blowfish algorithmic rule with the utilization of a duplicate cloud storage.

An overview of data storage and retrieval techniques in the cloud is presented in [5]. To protect data from leaks, it is stored in encrypted form in the cloud. Therefore, [5] also investigates techniques for searching for encrypted data in the cloud. In [6] a series of security protocols is presented which guarantee the protection of customer data in cloud computing infrastructures. The approach is based on secure cryptographic coprocessors in order to provide a reliable and isolated execution environment within the cloud computing. Data from the cloud after a partial loss is shown in [7-8].

III. PROPOSED METHODOLOGY

The proposed application uses hash functions for integrity maintenance, Blowfish algorithm for privacy protection, and TPA MD5 for identity verification.

2.1 Blowfish

It is a symmetric cryptographic technique that is used in popular applications. It is used with a large number of cipher blocks and cipher products along with SplashID, the full algorithm could not be broken, it is a fast block cipher for general use, which makes it an ideal product like SplashID that works on wider processors used in smartphones and laptops are scanned.

It is used to replace the free classic DES. Since Blowfish is associated with an alternate process, it consists of a 64-bit block size and a 32-448-bit key length. It is defined as a 16-round Feistel cipher and uses massive key-dependent S-boxes. The same goes for the arrangement of CAST-128, which uses S-boxes.

2.2 MD5

The MD5 message digest algorithm is a widely used hash function that can generate a 128-bit hash value. Although MD5 was originally developed for use as a cryptographic hash function, it has been found to have a wide range of security flaws. The checksum is used to check the integrity of the data, but only to prevent accidental damage. It is also suitable for other non-encrypted purposes, such as Define partitions for specific keys in a partitioned database.

The system architecture of is shown in figure 1 and its modules are mentioned as below

1. ERP (Patient Health Records)
2. Cloud Middleware
    - CSV Parsing
    - CSV Conversion
    - SOAP Configuration
3. Encryption
4. TPA

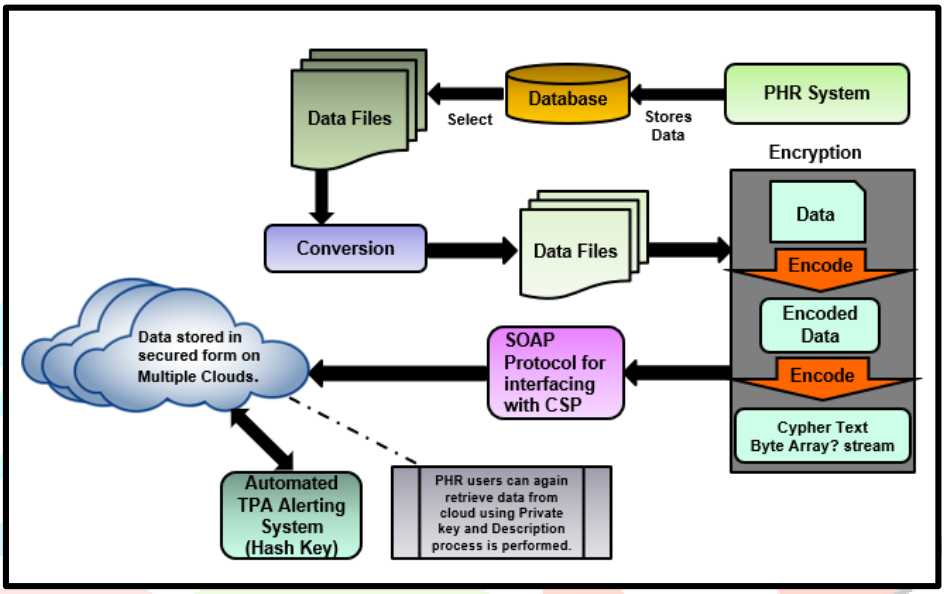

Fig. 1-Proposed System Architecture

The modules of the proposed system are as follows:

1. **ERP (Patient Health Record)** The user can be an ERP system or a commercial organization that uses the cloud for data storage. An ERP system runs on a variety of computer hardware and network configurations and typically uses a database to store information. The transition from ERP to a cloud-based model has been relatively slow. Some functions will be moved to the cloud for data storage and calculation.
2. **Cloud Middleware** It is a unit that is managed by a cloud service provider (CSP) to provide data storage services and has significant storage space and computing resources. In this system we implement the middleware that acts as a server. This middleware only needs one system to perform data encryption operations. This definitely reduces the hardware requirements like the server, your cooling system and the space for the server, and above all high costs are reduced.
    - **CSV conversion** After parsing, the CSV file is generated from the database. Because CSV files are referred to as "comma separated values," uploading to the cloud is easy as it reduces file size and offers double security.
    - **CSV parsing** CSV parser is used to decrypt the text. Defines a set of rules for encoding documents in a format that can be read by humans and machines. Keeps the layout of CSV files unchanged as they are uploaded to the cloud.
3. **SOAP protocol** SOAP, originally described as "Simple Object Access Protocol" [6], is a protocol specification for changing the registry that was set up when implementing Internet services in computer networks. The message format uses Comma Separated Value (CSV) files and other application layer protocols are generally used. This SOAP protocol is used to interact with the cloud service provider (CSP).

4. **Encryption** This system accepts normal data and then encodes it. Once encoded, encrypted data is provided in ciphertext [9] which is processed when this system actually processes the organization's ERP database or transactional data. Time as encrypted fields, records, rows or column data in a database. As soon as the encryption is carried out, CSV Parser decrypts the ciphertext. Data protection so that no unauthorized person can see, change or delete the ERP data. The set of rules of the Blowfish algorithm is used for the encryption process.

5. **External Auditor (TPA)** An optional TPA [1] who has experience and skills that users do not have, relies on them to assess and detect the risk of cloud storage services on behalf of users who request them. able to effectively examine cloud data storage without replicating data and without creating additional online burden on users. In addition, TPA notifies users if another person tries to hijack data or gain unauthorized access to data in the cloud storage. Once the data is securely stored in the cloud and the user or the ERP wants to retrieve this data, the user or the ERP can use the private key and retrieve the data from this cloud.

IV. RESULTS AND DISCUSSION

In this section we describe the experimental setup of the proposed approach in terms of secret key generation and communication and computing costs. We compared these results with traditional approaches to sharing patient health data on various data protection parameters. We calculated the performance of the proposed approach against existing approaches in terms of processing health data for cloud patients.

Most security techniques and protocols have their cryptographic strength expressed in terms of the number of bits (keys) an attacker would have to guess in order to break into the system. For example, if the attacker starts with partially predictable key material, this indicates the weakness of security systems regardless of the algorithm or protocol used. In the proposed scheme, patient data is collected from client devices ERP (Patient Health Record) and created CSV Data processing files; This encrypted information is transmitted to a remote client computer by processing via the SOAP protocol via CSP. The data is securely stored in the cloud after the request received from the TA client has been activated and reported to the system. ERP users can retrieve data from the cloud with a private key and the decryption process is complete.

The hash code generated is a 16-byte hexadecimal code that is stored in the database. The content is also converted from binary to hexadecimal format, which is available in encrypted format by the Blowfish algorithm. For users, it will be available on the cloud server. The database contains tables with information on user registration details, user login details, approval / denial status details of the user request.

User uploads the files, he/she has full authorization to revoke the keys if necessary. The request is submitted and only if the request is approved can the file be accessed using the private and public keys sent after the request was approved.

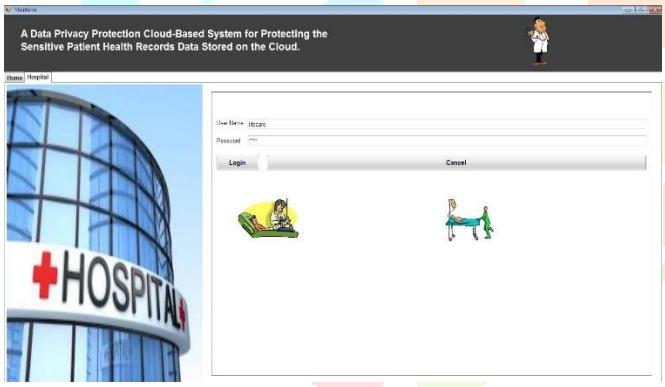

Fig. 2- **Login**: This is login form, Hospital can login for patient login and uploading patient details i-e PHR

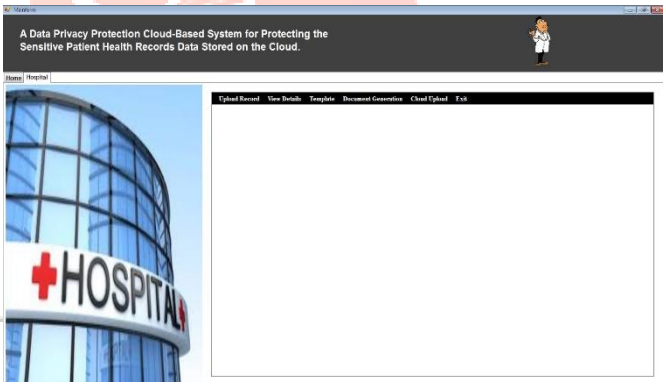

Fig. 3- **Menu Form**: This is a Menu Form in which user can view options for patient details, registration, cloud upload, and etc.

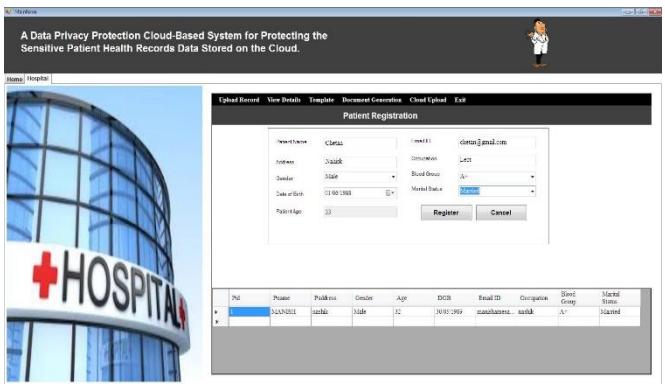

Fig. 4- **Patient Registration**: In this patient details of registration is been done.

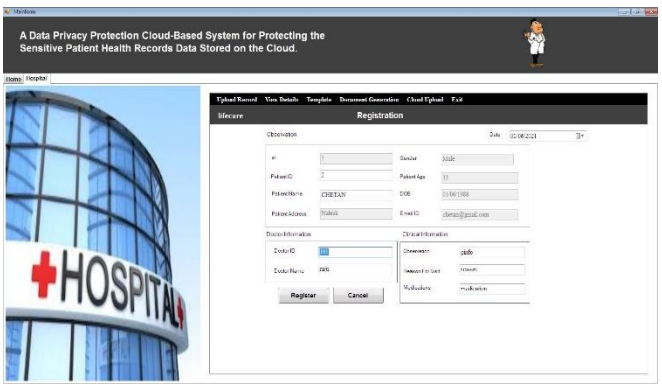

Fig. 5- **Patient Details:** In this patient clinical details is been added i.e., disease, prescription, doctor name etc.

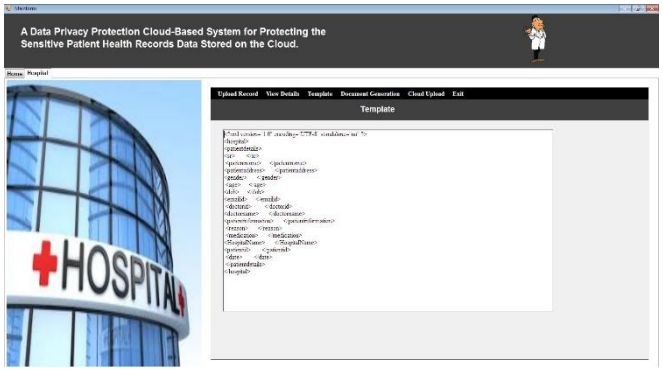

Fig. 6- **Document Template:** In this form record are been converted into fix template in which data is uploaded.

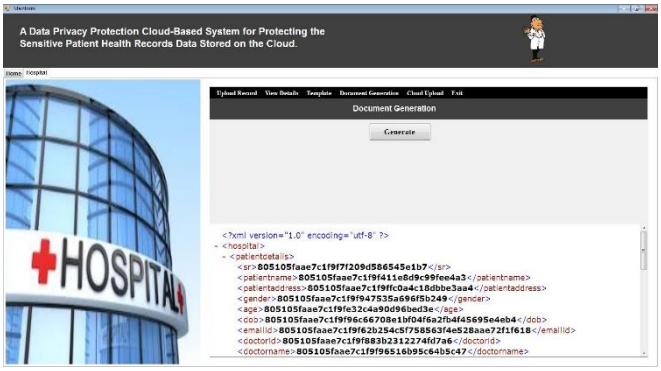

Fig. 7- **Document Generation:** Records which are added are been encrypted and converted in specific document.

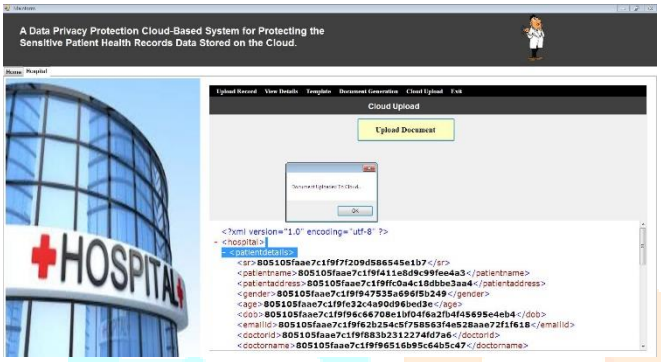

Fig. 8- **Cloud Upload:** After encrypting document record document is been uploaded onto cloud. At time of uploading hashing or signature of file is been generated.

Fig. 9- Data Owner Main form: This is main of data owner; Data owner can view and validate data.

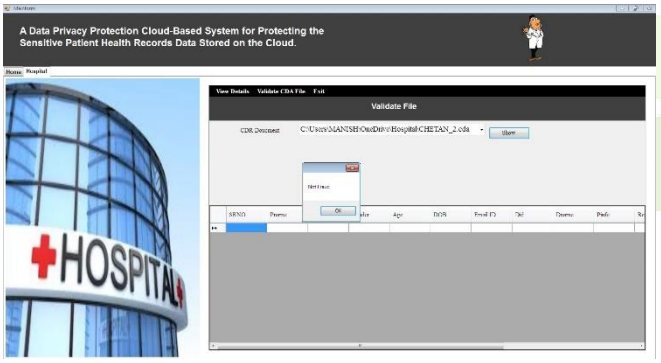

Fig. 8- **Document Validation:** In this form hashing algorithm is been executed and compare with signature stored in database. If signature does not match system will show fraud else system will show no fraud.

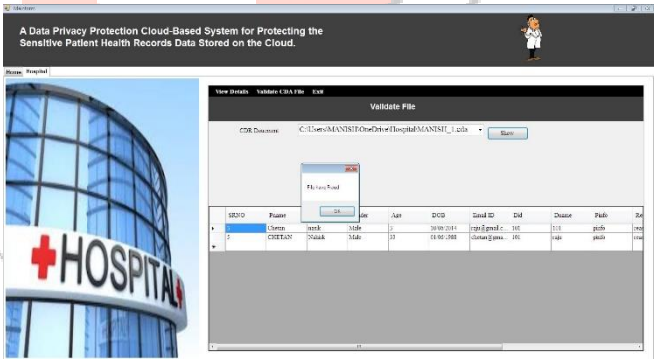

Fig. 8- **Document Validation Fraud:** In this form hashing algorithm is been executed and compare with signature stored in database. If signature does not match system will show fraud else system will show no fraud.

V. CONCLUSION

It is important to transfer data securely while maintaining its privacy and protection. The proposed work uses the cloud service, which can also be accessed from remote areas at any time. The proposed work aims to ensure data privacy and protection. These two criteria are successfully achieved with the two efficient algorithms: MD5 and Blowfish. Here privacy is achieved with encrypted Blowfish. The validation takes place via MD5.

Security is one of the problems hindering the rapid adoption of cloud computing technology in healthcare. The strengths and benefits of cloud computing far outweigh the dangers and threats. The confusion is that safety is negatively proportional to the consumer In other words, the clearer the security measures, the less comfortable consumers are and, as a result, they are less inclined to use the cloud service. data stored in the cloud. It is supported to split a certain file into several parts and to save each part after encryption and to sort the order of the parts with a special cloud provider. the knowledge to decrypt and rearrange the parts of the file is stored in separate locations with the customer. There are no additional costs as the total storage size remains the same compared to storing the file with a cloud provider. Customers in order to benefit from all security measures of the cloud provider and at the same time to pay attention to the security and data protection of their data.

The data cannot be prone to any kind of attacks even if the one-time keys got leaked, because, after every single usage of the public and private key, they automatically get revoked before the next key request. The future work can be extended towards safe transferring of video files.

REFERENCES

[1] **A**li Sakr1, Elias Yaacoub1,2, Hassan Noura1, Mohammed AlHusseini2, Khalid Abualsaud3, Tamer Khattab4, Mohsen Guizani5, "A Secure Client-Side Framework for Protecting the Privacy of Health Data Stored on the Cloud", 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM),.

[2] A. Bhardwaj, S. Chaudhary, and V. K. Sharma, "Biometric Authentication-Based Data Encryption Using ECG Analysis and Diffie–Hellman Algorithm," in Advances in Intelligent Systems and Computing, 2019, doi: 10.1007/978-981-13-5934-7_46.

[3] M. A. M. Isa, H. Hashim, S. F. S. Adnan, N. N. Mohamed, and Y. F. Alias, "Side-channel security on key exchange protocol: Timing and relay attacks," Indones. J. Electr. Eng. Comput. Sci., vol. 11, no. 2, pp. 688–695, 2018, doi: 10.11591/ijeecs.v11.i2.pp688-695.

[4] H. Aghili, "Improving security using blow fish algorithm on deduplication cloud storage," in Lecture Notes in Electrical Engineering, 2019.

[5] Md Hussain Ahmad and M. Madhava Tripathi, "Development of Encryption and Decryption Technique To Secure the Confidential Data," Int. J. Adv. Res. Comput. Sci., vol. 9, no. 2, pp. 60–63, 2018, doi: 10.26483/ijarcs.v9i0.6138.

[6] J. Kaur and S. Sharma, "HESSIS: Hybrid Encryption Scheme for Secure Image Sharing in a Cloud Environment," in Communications in Computer and Information Science, 2019, doi: 10.1007/978-981-13-3143-5_18.

[7] W. Itani, A. Kayssi and A. Chehab, "Privacy as a Service: Privacy Aware Data Storage and Processing in Cloud Computing Architectures", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2009), p.p. 711-716, Chengdu, China, Dec. 2009.

[8] U. S. Department of Health and Human Services, Health Information Privacy; URL [Accessed Dec. 7,2017] https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html

[9] G. Kurikala, K. G. Gupta, and A. Swapna, "Fog Computing: Implementation of Security and Privacy to Comprehensive Approach for Avoiding Knowledge Thieving Attack Exploitation Decoy Technology", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 2, no. 4, p.p. 176-181, Aug. 2017.

[10] Mell P., Grance T. The NIST Definition of Cloud Computing [Recommendations of the National Institute of Standards and Technology-Special Publication 800-145] Gaithersburg, MD, USA: NIST; 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800- 145.pdf.

[11] M. M. Wong, J. Haj-Yahya, S. Sau, and A. Chattopadhyay, "A New High Throughput and Area Efficient SHA-3 Implementation," Proc. - IEEE Int. Symp. Circuits Syst., vol. 2018-May, no. 1, 2018, doi: 10.1109/ISCAS.2018.8351649.

[12] J. Sen Teh, K. Tan, and M. Alawida, "A chaos-based keyed hash function based on fixed point representation," Cluster Comput., vol. 22, no. 2, pp. 649–660, 2019, doi: 10.1007/s10586-018- 2870-z.

[13] Md Hussain Ahmad and M. Madhava Tripathi, "Development of Encryption and Decryption Technique To Secure the Confidential Data," Int. J. Adv. Res. Comput. Sci., vol. 9, no. 2, pp. 60–63, 2018, doi: 10.26483/ijarcs.v9i0.6138.

[14] Cloud foundry, "Cloud foundry," 2017, https://www.cloudfoundry.org/.

[15] Amazon, "Amazon EC2," 2017, https://aws.amazon.com/ec2/