ZKG INTERNATIONAL

ISSN: 2366-1313

ENHANCING DATA SECURITY IN CLOUD USING BLOCKCHAIN TECHNOLOGY

[1]Mr. J. RAMESH, [2]M.SAI KUMAR, [3]B. UPENDHAR, [4]K. ABHIJEET SURYAVAMSHI

[1]Assistant Professor, Dept.of IT, TKR College of Engineering & Technology, Meerpet, Hyderabad, rameshjarapala@tkrcet.com

[2]BTech student, Dept.of IT, TKR College of Engineering & Technology, Meerpet, Hyderabad,

saikumarmadugula905@gmail.com

[3]BTech student, Dept.of IT, TKR College of Engineering & Technology, Meerpet, Hyderabad,

bashettiupender@gmail.com

[4]BTech student, Dept.of IT, TKR College of Engineering & Technology, Meerpet, Hyderabad,

abhukamlekar@gmail.com

Abstract: *Daily huge amount of data is exchanged and loaded on a cloud into different sectors one of which is the health sector. Data exchanged between the patient and doctors need to be secured to gain patients trust. Blockchain is a mechanism to secure data in a more advanced way. Blockchain stores data into chunks that make it complex to decode, which will help provide an extra layer of security. Hash chain is the most reliable part of the blockchain that will help keep the data unreadable. This data can be secured by using a blockchain mechanism at the backend of any hospital website to store the reports of the patients and maintain a two-way authentication for doctor's access to the reports. Using the concepts of dividing data into chunks and establishing an inter-link between each chunk is one of the aspects of blockchain which is implemented on the hospital generated data to inherit blockchain mechanism.*

Keyword: *Blockchain, cloud computing, Security, AES algorithm, Hash code*

I. INTRODUCTION

Cloud computing is the recent arising technology of IT industry to solve the problems and difficulties of business database services such as storage capacity, performance, stability, security, load and many other issues. Cloud storage was used to provide the cloud-based data storage platform. The computing tasks are distributed to a large number of computer systems, so that all applications can access the calculation capability, storage space and software services [1]. Definition of Cloud computing changes from professionals to professionals and from individual to individual. Everyone has their own way of defining cloud computing. e primary goal of cloud computing is to offer the organisation services that are both affordable and effective. Infrastructural and data management costs are decreased as a result. vast services are offered by cloud providers. How to secure, safeguard, and process data is the core objective of cloud computing. AES Algorithm is of the out sourced data in cloud environment the “effective automatic data reading protocol” and multi-server data compression algorithm. AES is an algorithm for performing encryption which is a series of well-defined steps that can be followed as a procedure. The original information is known as plaintext, and the encrypted form as cipher text. Plain text converted into the cipher text, that is not in the readable format. To convert this cipher text into plain text there is reverse technique that decryption technique it will convert cipher text into the plain text means in readable format. Blockchain plays a key part in the decentralised peer-to-peer system that is driving the rapid development of information technology in security. Blockchain technologies like the hashing algorithm, public/private key encryption, and transaction ledgers make this possible. Every piece of data is kept in a different decentralised place. If hackers attempt to access it, they first obtain encrypted data and then only a portion of the file, not the entire thing. This protects documents stored in cloud storage powered by blockchain. Blockchain is having a good effect and making it easier, faster, and more reliable to use storage, transactions, and business operations. The way forward is to combine blockchain and cloud to benefit from increased security and decentralisation, which improves authorisation, privacy, and efficiency[2].

Despite using certain frameworks, we have implemented the idea through hard coding. Each report is divided into chunks and these chunks need to be secured to maintain the integrity of data. Each of the chunks is encrypted through AES the key generation algorithm generates the public key (PK), the master key (MK), secret key (SK) of the user. There is a K number of users in group sharing data. Master, the user is the owner of data. So, all the users can access and modify the shared data in the cloud. TPA performs data integrity auditing for modified data of the user. Key Generation as the part of the setup algorithm generates public keys (PK), master keys (MK) of the system, and secret key (SK) of users. In our design each user will have their secret key for data modification Key generation is a technique which is used to store the data in a different methodology and mainly the public key algorithm known as RSA plays a vital role in key generation technologies such as single shared key uses symmetric key algorithm through which data will be stored very secretly Since the public key algorithm uses two keys namely public and a private key and that public key is made as visible to one end user so that they can use that public key to encrypt the data and another end-user can decrypt the data using their private key[3].

In some conditions, the keys have been generated using the random number generator technique, and it is very efficient that hackers cannot easily guess the keys and provide strong security. the major focus in our paper is about the healthcare data. Hospitals generate a large amount of confidential data and especially every healthcare center needs to maintain HIPAA rules. Here we are using a blockchain mechanism to the data that's been uploaded by the patients regarding their diseases and that data is then secured through blockchain mechanism. This security mechanism will be the backend processing of any hospital website, Recently, a few attempts started considering more realistic scenarios by allowing multiple cloud users to modify data with integrity assurance. Nevertheless, these attempts are still far from practical due to the tremendous computational cost on cloud users, especially when high error detection probability is required by the system. We used Amazon Cloud Storage service S3 for storing data divided into chunks in the form of buckets.

II. LITERATURE SURVEY

In [4] Block chain being a foundational technology impacting and attracting a wide range of applications has become predominant in solving the problem of privacy preserving and security in multitude sectors that is under the control of the government and the private. The paper also presents the security and the privacy mechanism using the block chain to prevent the misuse and the corruption in the sharing of huge set of data generated from the judiciary, security, legislature, commercial code registries. The proposed system enables reliability and the trust in the data sharing in the communication channels utilizing the block chain with the RSA digital signature. The proposed system is simulated as a java programming version to evince the enhancement in the latency in the sharing of the information's along with the privacy and the security.

In [5] Due to their specific features, blockchains have become popular in recent years. Blockchains are layered systems where security is a critical factor for their success. The main focus of this work is to systematize knowledge about security and privacy issues of blockchains. To this end, we propose a security reference architecture based on models that demonstrate the stacked hierarchy of various threats as well as threat-risk assessment using ISO/IEC 15408. In contrast to the previous surveys, we focus on the categorization of security vulnerabilities based on their origins and using the proposed architecture we present existing prevention and mitigation techniques. The scope of our work mainly covers aspects related to the nature of blockchains, while we mention operational security issues and countermeasures only tangentially.

In [6] A cooperative network defense is one approach to fend off large-scale Distributed Denial- of-Service (DDoS) attacks. In this regard, the Blockchain Signaling System (BloSS) is a multi-domain, blockchain-based, cooperative DDoS defence system, where each Autonomous System (AS) is taking part in the defense alliance. Each AS can exchange attack information about ongoing attacks via the Ethereum blockchain. However, the currently operational implementation of BloSS is not interactive or visualized, but the DDoS mitigation is automated. In real-world defense systems, a human cybersecurity analyst decides whether a DDoS threat should be mitigated or not. Thus, this work presents the design of a security management dashboard for BloSS, designed for interactive use by cyber security analysts.

In [7] With the development of cloud computing technology, developed countries including the U.S. are performing the efficiency of national defense and public sector, national innovation, and construction of the infrastructure for cloud computing environment through the policies that apply cloud computing. Korea Military is also considering that apply the cloud computing technology into its national defense command control system. However, only existing security requirements for national defense information system cannot solve the problem related security vulnerabilities of cloud computing. In order to solve this problem, it is necessary to design the secure security architecture of national defense command control system considering security requirements related to cloud computing. This study analyze the security requirements needed when the U.S. military apply the cloud computing system. It also analyze existing security requirements for Korea national defense information system and security requirements for cloud computing system and draw the security requirements needed to Korea national defense information system based on cloud computing.

In [8] Based on the proposed group data sharing model, we present general formulas for generating the common conference key IC for multiple participants. Note that by benefiting from the (v, k + 1,1)-block design, the computational complexity of the proposed protocol linearly increases with the number of participants and the communication complexity is greatly reduced. In addition, the fault tolerance property of our protocol enables the group data sharing in cloud computing to withstand different key attacks, which is similar to Yi's protocol.

In[9] In this paper, they proposed a framework for secure storing of data on the cloud-based social networks. The framework encrypts the data before storing it in the cloud, and the data is decrypted only with the private key of the user, making the data secure in the cloud. The proxy re-encryption scheme is used to re-encrypt the data to make it more secure.

III. PROPOSED SYSTEM

The overall working of the proposed system will have a UI for any hospital through which the patients can book the slot for check-up and doctors can view those requests. Doctors need to request the patients for downloading the report which requires an OTP that's been sent on to the patient's email. As for storage once the patient uploads the report is divided into chunks of the file and these chunks are encrypted using AES, these chunks of data are distributed among 2 buckets. These buckets store the chunks of file randomly distributed among them and have an interlink to form a chain within the chunks.

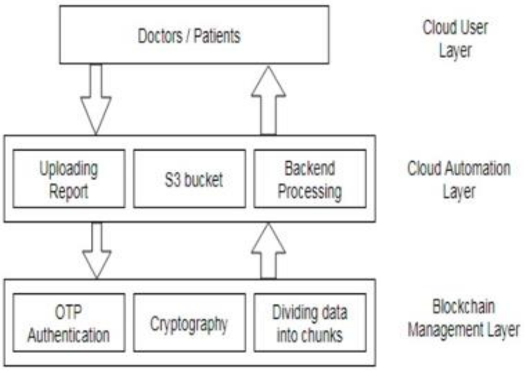


Fig.1 Proposed method

The proposed work divided into various stages

Data Chunks: Dividing data into chunks will increase the data integrity, by making the data more complicated at the backend as a single report will be broken into smaller files each containing some part of the report.

Cryptography: AES Encryption fill help secure the data and maintain confidentiality, each chunk of the report will be encrypted through AES individually

Inter-linking: These chunks of the report need to have some sort of connection to maintain the authenticity of the data this can be achieved through linking each chunk with the next chunk following the concept of chaining of blockchain.

Consensus: Approval from the patient side should be maintained to achieve trust between doctor and patient; these can be done by maintaining OTP verification from the patient's side for the doctors to download the report.

S3 buckets: Storage of these chunks of data needs to be in a secure environment and what's better than using a cloud environment, using S3 buckets to maintain the storage of file chunks. S3 makes storage more reliable and durable.

The overall working of the proposed system will have a UI for any hospital through which the patients can upload their reports and doctors can view those reports. Doctors need to request the patients for downloading the report which requires an OTP that's been sen t on to the patient's email. As for storage once the patient uploads the report is divided into chunks of the file and these chunks are encrypted using AES, these chunks of data are distributed among 3 buckets that are formed using S3 a storage service by AWS. These buckets store the chunks of file randomly distributed among them and have an interlink to form a chain within the chunks

MODULES

Transport Layer Security (TLS)

TLS is a protocol that provides secure communication over the internet. It uses AES encryption to protect data during transmission. By using TLS, you can ensure that your data is protected from eavesdropping and tampering.

Encrypted File Systems (EFS)

EFS is a feature of some operating systems that provides transparent encryption of files on disk. By using EFS, you can ensure that your data is protected even if the cloud provider's physical security is breached.

Key Management Systems (KMS)

KMS is a service that allows you to securely manage encryption keys. By using KMS, you can ensure that your encryption keys are protected from unauthorized access.

Secure Sockets Layer (SSL)

SSL is a protocol that provides secure communication between web browsers and servers. It uses AES encryption to protect data during transmission. By using SSL, you can ensure that your data is protected from eavesdropping and tampering.

Virtual Private Networks (VPNs)

VPNs allow you to establish a secure connection between your computer and a remote server. By using VPNs, you can ensure that your data is protected from interception and tampering

Data at Rest Encryption

Encrypting data at rest refers to encrypting the data when it is stored in the cloud. This ensures that even if someone gains unauthorized access to the cloud storage, they will not be able to read the data without the encryption key.

SYSTEM ARCHITECTURE

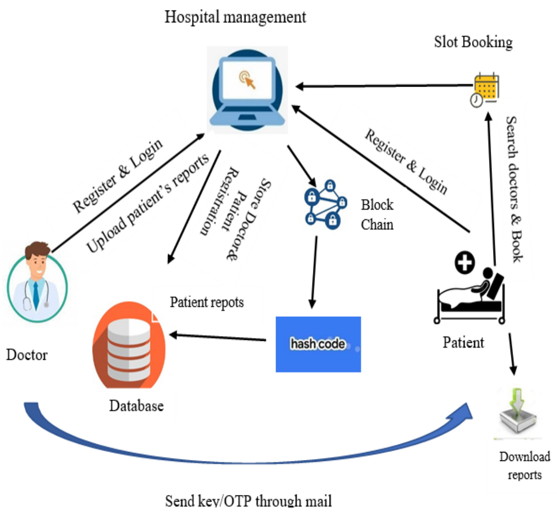


Fig.2 System architecture

IV. IMPLEMENTATION

Doctor

Doctor needs to be register and then login in to the website. After login they can view the all slots are booked by patients. Based on the following dates booked by the patients, doctor will provide the check up. After completion of the check up they can upload the patients reports. Those reports are stored in the database in the form of blocks. The uploaded reports will be divided in to chunks and each chunk is assigned with a hash code.

Patient

Here patient can register and login to the website. After login he/she can search the doctors based on their specialization. If the required doctors are available then the patient will book the slot. After the completion of patients checkup by the concerned doctor, the doctor will send the reports in an email which consists of a key/ OTP , the patient will download the reports.

ALGORITHM

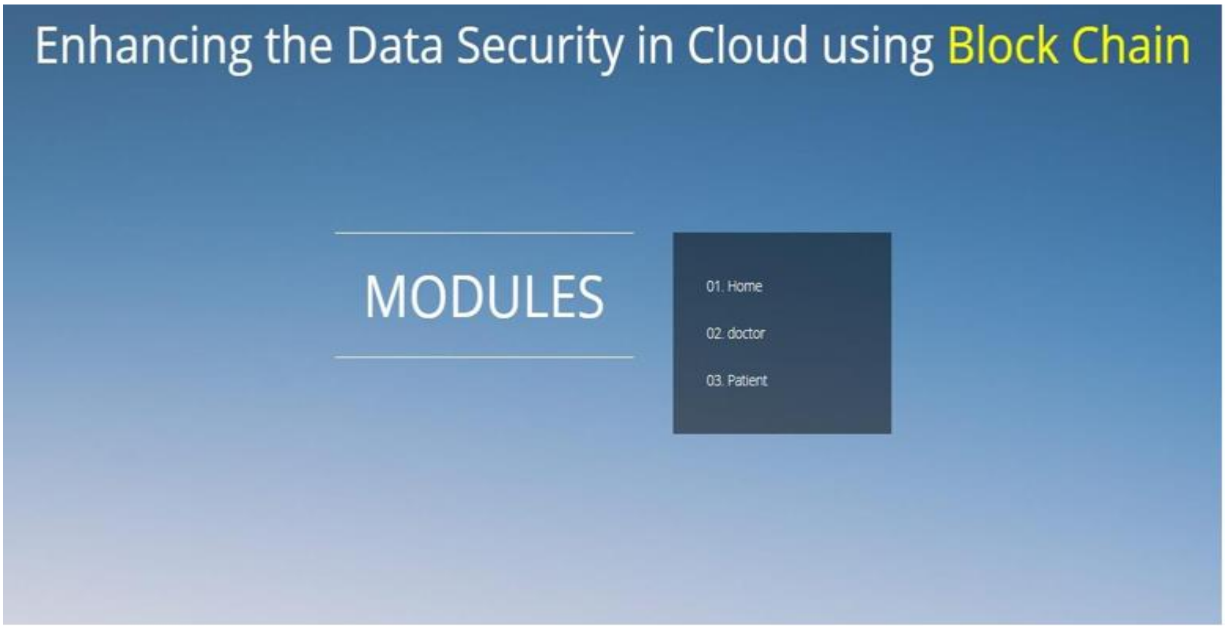
The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data The data to be encrypted. This array we call the state array.

Following AES steps of encryption for a 128-bit block:

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext). Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.
- Copy the final state array out as the encrypted data (ciphertext).

The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others. The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so we first convert the 128 bits into 16 bytes. We say "convert," but, in reality, it is almost certainly stored this way already. Operations in RSN/AES are performed on a two- dimensional byte array of four rows and four columns. At the start of the encryption, the 16 bytes of data.

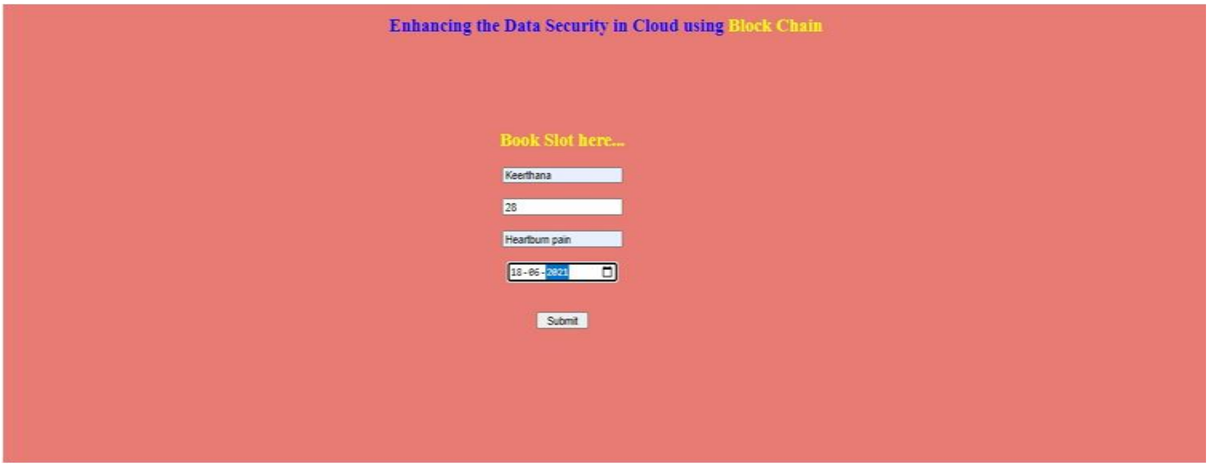
V. RESULTS



Enhancing the Data Security in Cloud using Block Chain

MODULES

Fig.3 Home page



Enhancing the Data Security in Cloud using Block Chain

Book Slot here...

Keerthana

28

Heartburn pain

18-06-2021

Fig.4 Slot Booking page

VI. CONCLUSION

We compare many types of photographs in this work, and the accuracy level of e results is really pleasing. The displayed the findings are 99 percent accurate. When compared to alternative approaches, this uses Jess memory space and takes less time to implement. Although cloud computing is the new emerging technology that presents a good number of benefits to the users, it faces lot of security challenges. AES encryption is the fastest method which has flexibility and scalability and is easily implemented. AES algorithm has a high level of security

ISSN: 2366-1313

because 128, 192 or 256-bit keys are used in this algorithm. It shows resistance against a variety of attacks such as square attack, key attack, key recovery attack and differential attack. Data can also be protected against future attacks such as smash attacks. AES encryption algorithm has minimal storage space and high performance without any weakness and limitation while other symmetric algorithms have weaknesses and differences in performance and storage space.

The proposed system can be developed in many different directions which have vast scope for improvements in the system These include

1. Increase the accuracy of the algorithm.

2. Improvising the algorithm to add more efficiency to the system and enhance its working 3. Updates are best to continue the legacy of any applications.

REFERENCES

1. Nakamoto S. Bitcoin : A peer-to-peer electronic cash system[J]. Consulted, 2008

2. International Conference on Advances in Computing, Communications and Informatics (ICACCI) Amita Kashyap, G. Sravan Kumar, Sunita Jangir, Emmanuel S. Pilli, Preeti Mishra “IHIDS: Introspection- Based Hybrid Intrusion Detection System in Cloud Environment”.

3. Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A. &amp; Kishigami, J.J (2015). Blockchain contract: A complete consensus using blockchain. 2015 IEEE 4th Global Conference on Consumer Electronics (GCCEP).

4. Matousek, K. (2008). Security and reliability considerations for distributed healthcare systems.2008 42nd Annual IEEE International Carnahan Conference on Security Technology.

5. Shen, J., Zhou, T., He, D., Zhang, Y., Sun, X., &amp; Xiang, Y. (2018). Block Design-based Key Agreement for Group Data Sharing in Cloud Computing. IEEE Transactions on Dependable and Secure Computing.

6. Zhe, D., Qinghong, W ., Naizheng, S., &amp; Yuhan Z. (2017). Study on Data Security Policy Based on Cloud Storage. 2017 IEEE 3rd International Conference on Big Data Security on Cloud (Big Data Security), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS).

7. Bharadwaj, D. R., Bhattacharya, A., &amp; Chakkaravarthy, M. (2018). Cloud Threat Defense-A Threat Protection and Security Compliance Solution. 2018 IEEE International Conference on Cloud Computing in Emerging Markets.

8. Suma, V. (2019). SECURITY AND PRIVACY MECHANISM USING BLOCKCHAIN. Journal of Ubiquitous Computing and Communication Technologies (UCCT), 1(01), 45-54

9. Praveena, A., and S. Smys. “Ensuring data security in cloud based social networks.” In 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA),vol. 2, pp. 289-295. IEEE, 2017.

10. Homoliak, I., Venugopalan, S., Hum, Q., &amp; Szalachowski, P. (2019). A Security ReferenceArchitecture for Blockchains. 2019 IEEE International Conference on Blockchain (Blockchain)