Cloud Server Security using Bio-Cryptography

Zarnab Khalid[1], Muhammad Rizwan[2], Aysha Shabbir[3], Maryam Shabbir[4], Fahad Ahmad[5], Jaweria Manzoor[6]
Department of Computer Science
Kinnaird College for Women, Lahore, Pakistan

***Abstract*—Data security is becoming more important in cloud computing. Biometrics is a computerized method of identifying a person based on a physiological characteristic. Among the features measured are our face, fingerprints, hand geometry, DNA, etc. Biometric can fortify to store the cloud server using bio-cryptography. The Bio-cryptography key is used to secure the scrambled data in the cloud environment. The Bio-cryptography technique uses fingerprint, voice or iris as a key factor to secure the data encryption and decryption in the cloud server. In this paper, the security of the biometric system through cloud computing is discussed along with improvement regarding its performance to avoid the criminal to access the data. Biometric is a genuine feature for the cloud provider. Cryptography algorithm will be explained using blockchain technology to overcome security issues. The blockchain technology will provide more protection through cryptographic keys to secure biometric data.**

Keywords*—*Cloud computing; biometrics; fingerprints; encryption and decryption methods; cryptography keys; bio-cryptography; blockchain

I. Introduction

Cloud Computing is mainly a spotlight of the computer industry today. Cloud computing is an evolving model with new aspects and capabilities, maintaining the data of cloud is dominant. There are many techniques and approaches to maintain the data and secure in the cloud server [1]. In a cloud computing environment, the entire data exist in a set of networked resources. Cloud service is available all around the world using standard network protocol accessible from every device with internet connection (laptops, mobile phone, tablets). Authenticating is necessary for validating one to part by an interactive party that is usually implemented in client-server side where sever needs to confirmed who is accessing their information and needs to be authenticated. The main drawback of cloud computing technology is lack of confidence they gained from possible receivers specially internet users [4].

Biometry technology provides verification of identity and sensitive security level, while in cryptography key management is a necessary for key storage. Biometric is combined with cryptography because biometry feature is admissibly unique, as a result bio-cryptography was put to secure the cloud server using key binding to create cryptographic key. Key binding is the main concept in bio-cryptography [2] that combines user biometrics with the existing cryptography keys to form biometric encryption process. Biometric is basically used for security and networking system.

The Cryptography key is entirely independent on biometrics. The main idea of cryptography is to avoid the unauthorized operations on documents, text ad storage base [3].

Cloud Computing Architecture comprehends components and subcomponents that are mandatory for cloud computing. The architecture contains front end platforms called clients, these clients are servers, e.g. Mobile laptop, printer, tab, etc. The back-end platforms are mostly servers for storage, database, software applications and operating system within a cloud and a network counting the internet, intercloud combines to form a cloud computing architecture. The front and the back end of cloud usually connect each other to form a network and is named as internet. If cloud computing has many clients then it is high demanded for a lot of storage data. The archtitecture of cloud computing has been shown in Fig. 1.

The Biometric system is raised its increasing and has become the promising way to identify users [7] and authentication methods based upon password, identification cards and is considered to be more reliable. The biometric system consists of three steps. The first step involves enrollment in which the user can store basic information about the user id and user number, then identifies an image of specific trait and check the specific characteristic being used e.g. fingerprint. The second step is to read information from the system. The system analyses the characteristics and perform actual comparison to match the pattern of given input. After comparison, the user can either accept or reject the procedure present in the file.

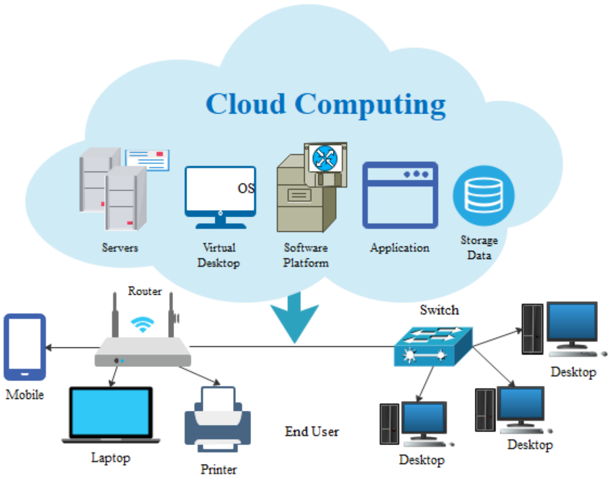

Fig. 1. Cloud Computing Arcitecture [7].

Cloud computing is an evolving model with new aspects and capabilities, maintaining the data of cloud is dominant. There are many techniques and approaches to maintain the secure data in the cloud server. Cloud computing undergoes many attacks and can be secured using methods and techniques to overcome the problems related to the security [12]. Cloud service is available all around the world using standard network protocol accessible from every device with internet connection (laptops, mobile phone, tablets) [13]. Cloud computing security is based upon authentication and verification of some parameters that can help in measuring the right amount of data security in the cloud server.

Biometry technology provides verification of identity and sensitive security level, while in cryptography the key management is necessary for storing key. [8] Inception and deception are two phases of network analysis to determine network traffic stream, biometric data is secured using secret key sharing among encryption and decryption parties. The original biometric data is extracted by generating a key. The Cryptography key is entirely independent on biometrics. [6]

The biometrics can secure passcodes more effectively [9] and authenticate the uniqueness in an individual to grant access to the computer or system using fingerprint scanner technology.

The Blockchain essential is an evolutionary internet protocol. It is an open source cryptography asymmetric mechanism and distributed architecture. Many aspects of technology are found in the blockchain peer to peer technology, cryptography [10] distributed over a network, the security of blockchain relies on these technologies. The Blockchain technology is completely different from traditional database structure. Peer to peer network that accomplished blockchain collectively following protocol for communicating inner-node and authenticating new nodes. Each block holds a valid transaction that is distributed over a network.

This blockchain technology uses a script to deal with the sudden pattern transaction in the system. Blockchain is made of three technologies private key cryptography, peer to peer network and blockchain's protocol. The blockchain is simply a cryptographically provable list of data [11]. The primary advantage of the blockchain technology is that data itself can be dispersed. The blockchain undergoes many attacks from third party to access the files in cloud server [14] and can be prevented by using technologies and blockchain security to protect the data from theft. In this paper cryptography keys will be discussed along with blockchain technology that will help in securing the biometric data in cloud server. Bigger blockchains user with more users has lower risk of getting attacked by the hacker because of the large number of complexities required to breach such a network

In Section II, Literature Review is discussed. In Section III, problem statement of the paper is deliberated. In Section IV, the proposed solution of the paper is elaborated and explained through biometrics, cryptography keys and blockchain technology that explain how the data is secure more effectively in the cloud server. In the end, Section V will designate the conclusion and discussion regarding the paper. The security of blockchain depends upon cryptography peer to peer technology. The Cloud server for storing information is given below to explain how the data is being stored and protected through encryption and decryption of cryptographic keys, identification through biometric technology and at last blockchain transaction that holds blocks of data. The data is stored forming chains inside the block. The data is processed to be fit in a block and each block is represented by using cryptographic hash. The architecture of securing data in cloud computing has been shown in Fig. 2.

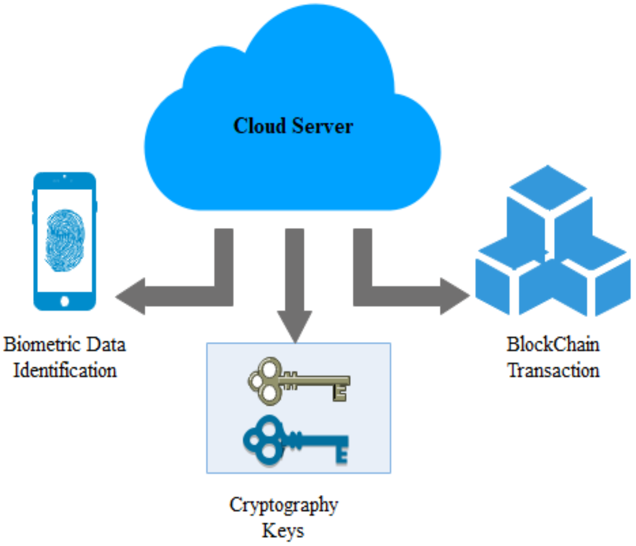

Fig. 2. Cloud Computing for Securing Data.

II. Literature Review

The last researchers finding and investigation have been written previously. Cloud computing security importance and techniques [1] are used to overcome data privacy issues and problems handled by cloud server provider. Author in [2] proposes two methods to decrease bio-cryptography computational complexity using fuzzy vault technique to rehearse error-correcting codes in the secret key. Author in [3] explains multiple methods to secure data using cryptographic keys and comparison between cryptography methods. Different methods are discussed to secure data using cryptography process. The multimedia data are high dismissal of large capacities and requires real time analysis for better results. Author in [4] proposed protective biometric identification scheme that can attack conspiracy tossed by the users and the cloud server. The proposed result can accomplish an essential level of protection by resisting the attacks and to provide lesser estimation costs in identification procedures. Author in [5] proposed user authentication points on bases of fingerprint authentication and comparing with previous method. Author in [6] used existing techniques to organize in different types of solutions. Using previous techniques error control methods in bio-cryptography will be discussed. Author in [7] proposed scheme is to secure cloud if the invader can falsify identification demand and to secure the cloud from the attackers and comparisons with previous protocols to get results more effectively. In [8], author provides evidence to detect cryptography procedures by their unique key exchange. The methods of generating cryptography protocols to detect high entropy data by the method of fingerprint were proposed. Author in [9] proposed extracting features and matching procedures through fingerprint system to secure hardware techniques, categorizes different part of including techniques for extracting its features and matching of the procedures. Author in [10] implements digital signature scheme through blockchain. A method to apply similar concept and data structure with distributed method was introduced. In [11], the author proposes unsolved problems of blockchain community. The problems were analyzing in ranges from organizing newer cryptography primitives on bitcoin to enable use-case privacy protection of file storage. In [12] various security threats are explained in cloud computed and needed to be resolved. In [13] cloud computing security is measured on bases of parameters. Parameters are recognized to measure the data security of cloud. Author in [14] explains many attacks on the blockchain and provides assured data derivation of cloud. Author in [15] proposes set of cryptographic protocols confirming privacy of cryptographic procedures with public and private keys.

The prototype system is implemented using smart bonds. The comparison between previous research work has been shown in Table I.

TABLE I. Comparison between Previous Research Work

Year	***Topic***	***Proposed Solution***	***Strength***	***Weakness***
2014	Methods of Reducing bio-cryptography algorithms [2]	A technique to rehearse error correcting codes in secret key	Using methods for reducing bio-cryptography algorithms and providing flexibility to reduce the errors for security	High consumption of computational resources, caused by various mathematical processing and the huge amount of data
2014	Bio cryptography Authentication in cloud sharing [4]	Providing essential level of protection by lessening the attacks	Novel implementation for bio-cryptographic infrastructure and recovery of shared storage encryption	Culpabilities for storing encryption key within cloud platforms Password security is not upgraded
2015	Bio-cryptography authentication protocol improvement [5]	Fingerprint authentication and previous method comparison	Biometric authentication is improved against the fake device attacker for stealing biometric data and password	A method proposed by a researcher that was weak against the attacker with high time complexity
2015	Security threats in cloud computing [12]	Security threats to be resolved in cloud	Examine the various security issues that are defenseless to the cloud computing and needed to be resolved	The cloud computing brings critical challenges that cannot be avoided by the consumer, if security of clouds is concerned
2017	Multimedia cryptography [3]	Multiple method to secure the data using cryptography keys and their comparison	Using bio-cryptography to enhanced security of data or image while transmitting, this will be efficient for improving multimedia data encryption	Multimedia encryption is hard to understand due to conversion of original data into another data
2017	Security and privacy on Blockchain [11]	Unsolved problem in blockchain community	*Cooperation between academia and blockchain community to resolved unsolved problems*	*Problem in security and privacy* *Research and problems related to industry to analyze glitches ranging from organizing new cryptographic primitives*
2018	Privacy-preserving biometric identification in cloud computing [7]	Secure the cloud if the invader demands false identification	Secures and offer high level of privacy protection. Real experiments on the Amazon cloud, over databases with different scopes	Tremendous amount of cost in the system that depends on conformist cryptographic primitives
2018	Blockchain access control system for cloud storage [15]	*Privacy of cryptography procedures with public and private keys*	*Blockchain provides security in the cloud sharing and access control over the data stored in the cloud without provider participation*	*Security and copyright issues,* *Transfer of file to other users,* *Problems for encrypting the data.*

III. Problem Statement

Bio-cryptography secures the data by encrypting and decrypting in the cloud server. As the security of cryptography keys are weak for remembering pass codes so a method is required to secure the data more accurately. Cryptography keys are not secure. There are many privacy issues regarding this procedure so a technique is needed to provide full protection in cloud server.

IV. Proposed Solution

To secure the data more accurately and precisely biometric-based cryptography is combined with the blockchain technology to secure the data in the cloud server. Cryptography keys are usually weak to secure large data. Blockchain technology uses the cryptography encryption and decryption keys to secure network and to store values in it. Blockchain is linked with public cryptographic key to protect the data from the hackers accurately. The data in the blockchain is stored in form of record or text file.

A. Methodology

In This paper we will provide security of data saved in cloud server by the blockchain technology that helps the cryptography keys to implement secure data. Blockchain is also an internet distributed database method based on distributed architecture, Asymmetric cryptographic component. Blockchain technique used advanced block as data component through which data is stored in the form of record, text file. Blockchain contains three elements, one for data storing, other one for hash value that works like fingerprint. Cryptography is the main part of the blockchain where transaction must be kept private. Methods to store data in cloud server using bio-cryptography and block chain have been shown in Fig. 3. When biometric data is encrypted and secured in blockchain, it cannot be altered. Even if somehow the data gets altered, the entire chain of the network is also changing accordingly, this mean at every alternation or change in data is tracked and absolutely no data will be lost because the user can always look through the previous versions of blocks to find out the difference in the latest version. In this process the user enters the data through biometric identification scanner the data is encrypted into the blockchain for security and decrypt into the cloud server. The following steps explain the procedure to store biometric data in cloud server with the help of cryptography keys and blockchain.

1) The digital image of fingerprint is pre-processed to recover the image quality. This enhanced image is approved through fingerprint algorithm to identify unique details. The details of recognizing unique features of fingerprints are known as minutiae. A template is generated after the post-processing of fingerprint image.

2) After the fingerprint detection the biometric data is encrypted using cryptography keys. The encrypted data is then passed through blockchain transaction, each block holds the data.

3) The data is secured more effectively using blockchain that is linked with cryptography storing information in a form of chunks forming a chain that can hold transaction of data.

4) The secured data is then decrypted using private key so it can be read more effectively.

5) All the secured data is stored in cloud server after decryption. The stored information is secured and can only be accessed by server and user.

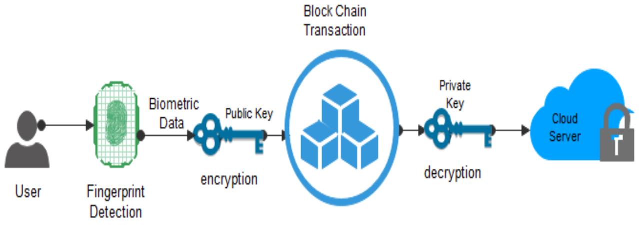

Fig. 3. Methods to Store Data in Cloud Server using Bio-Cryptography and Blockchain.

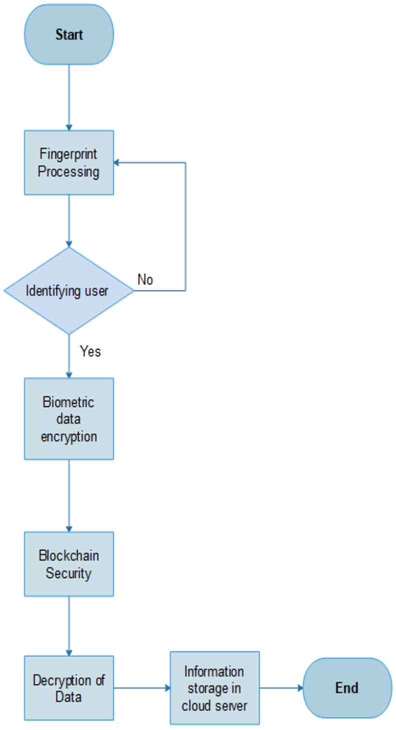

Fig. 4. Flowchart of Proposed Solution.

Flowchart of the following methodology is illustrated in Fig. 4. The flow chart describes the procedure to secure the data in the cloud server using cryptography and blockchain.

B. Biometric

Biometric is used in computer science for identification and access control. Biometric identification is calculable characteristics to identify distinctiveness. Biometric is identified by behavioural characteristics that includes fingerprint, veins, palm, DNA, iris recognition. A secure way to authenticate its user is to ensure functionality of data and data stored in cloud server biometric authentication is used secure the cloud and its data. Biometric is not n new technology nowadays but many of them neglects its unused potential. This Technology is growing rapidly. Organizations are adopting biometric to update passports. Biometric system can be updated in two methods verification and identification, for identification none of the approaches are claimed from the user while the goal of verification is to control whether the person is the one to be claimed.

Biometric is basically used for security and networking system. The biometric system has methods for identification linking PIN numbers and passwords. A fingerprint is a pattern of ridges on the surface of fingertip. The pattern of distinct remains unchanged throughout life. The fingerprints pattern is also unique in an individual. The details of fingerprint image are scanned into biometric system including the amount of pressure applied, dryness of skin or presence of any cuts or other deformities present on fingertip. Biometric are making smart phone more useful and might be a key for helping others by protecting the data with growing internet of things. The connected devices (laptops, computers, tablets) can be measured and the profile can be derived from biometrics from the resulted data. Biometric system contains three different components, sensor that records the information, a computer for storing biometric information, a software that connects computer hardware to the sensor. Biometric is in a form of identification and access control in computer science. Fig. 5 shows the working of finger identification through biometrics.

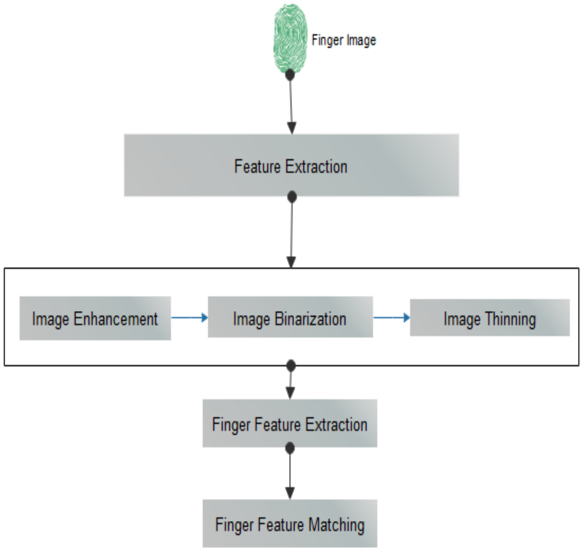

Fig. 5. Working of Finger Identification Through Biometrics.

C. Blockchain Technology

Blockchain provides a distributed, absolute data store that can be used across network of users. It is a distributed database that supports continuously increasing list of transaction information accounts, cryptographically protected from meddling and reviewing. The transaction data is kept in the blockchain. Blockchain consists of three elements first for data storage, second one is used as hash value that works like fingerprint and always unique to identify the block. The process of adding new block to blockchain by transaction of hash verification is known as mining. The new added block is linked with previous block. The third element is hash of previous block is chain of blocks to make blockchain more secure. The main drawback of blockchain is high consumption of hardware, energy and time required for mining process.

Blockchain has surged from a technology with slight applications associated with digital currencies. The security in blockchain is important to protect from the attackers. The data is protected through blockchain and kept in the cloud server. The data is stored forming chains inside the block. The data is processed to be fit in a block and each block is representing by using cryptographic hash usually known as digital fingerprint. When underlying cryptographic algorithms are broken, the impression of blockchain is analysed. The structure of the blockchain is given below. The blockchain is the underlying cryptographic protocol; each technology of blockchain is a factor to achieve the requirements. The security of cryptographic hash functions is essential part for the security of blockchain and its nature should be secure for a very long time. The blockchain technology used the chunks of data to store the data in it and to provide security of data by chaining them. Cryptography is the main essential for blockchain privacy where transaction needs to be private. The industrial benefits of blockchain are to improve discoverability, reduce costs and complexity and can be trusted in keeping records of files. Blockchain increases accessibility, improve efficiency in business networks. The structure of Blockchain has been shown in Fig. 6.

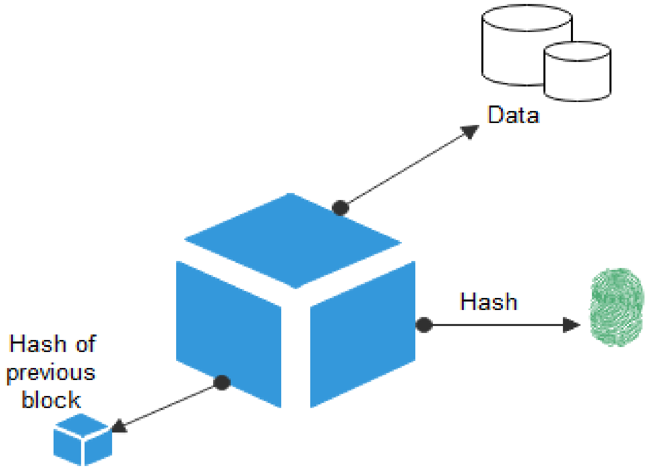

Fig. 6. Structure Diagram of Blockchain.

Blockchain is composed of three core parts: block, chain and network

1) Block: The block in blockchain is the main core of blockchain. A list of transaction recorded into a report over a given time. The size event and activation are different for every blockchain. Blockchain controls the movement of their token. The block header contains last block hash, transaction, time, target and version that describes the structure of the data inside the blockchain. When a block is completed it creates a unique secure code, that is tied with next block, creating chains of block.

2) Chain: The hash that links one block to another, chains them together. It is most difficult thought to perceived in blockchain. The hash in block is created from data from previous block. The hash is fingerprint of that data and links blocks in order. Hashing increases the security of the data. Hash pointers are where the blockchain sets itself in terms of certainty as pointers not only contains address of previous block, but also hash data of the block for attaining blockchain.

3) Peer to peer network: The network composes of nodes. The nodes work as a computer running an algorithm that secures the network. Each node contains entire records of transaction that are recorded in blockchain, in case of full node the whole blockchain is copied into the device, while device is being connected to the network. Peer to peer network in blockchain differs from traditional client-servers model, as there is no central point of storage and information is constantly shared, recorded between all applicants of the network.

D. Cryptography Algorithm

The Cryptography key is completely independent on biometrics. Cryptography algorithms include public and private keys for encryption and decryption of data. Bio-cryptography is used to avoid scrambling data in the cloud environment. Biometric authentication identifies users on the basis of their behavioral characteristics. Cryptography algorithm keeps data safe and secure when communicating through a network. Cryptography algorithm alters the data from readable form to a protected form. Cryptographic keys keep authentication and keep information private. Cryptography is used to secure information from unauthorized revelation. It has two fundamental types symmetric and asymmetric and has various properties like length and depends on proposed functions.

Cryptography converts ordinary information into scrambled incomprehensible clutter. This process of conversion is called encryption. The second process of cryptography is decryption which takes the cyphertext and recreates the plain text. The process of encryption and decryption is controlled by the key. The key is shared between two communicating parties. A technique derived from mathematical concepts and rule-based calculation known as algorithm that transfer messages that are hard to cipher so cryptography algorithms are generated for protection of data privacy, web surfing on internet and deliver confidential statements [16].

Cryptosystem uses a set of cryptographic algorithms to encrypt and decrypt messages among computer system, devices including smartphones and other applications. One algorithm is used to encryption; another algorithm is used for message authentication and another one for key exchange.

The process is embedded in protocols and run on network systems and operating systems, involving public and private key generation, message verification and key exchange [17]. Process of cryptography has been shown in Fig. 7.

1) Symmetric key encryption: Symmetric key is also known as private key. In this encryption a secret key is used for encryption and decryption. In the encryption process the information is locked using cryptography and can only be accessed by the user and server. The key is advanced by either the client or the both side (client and server). Distribution of keys is a big problem in this technique as encryption and decryption of data is done by a single key. Symmetric key is much faster than asymmetric encryption. Symmetric key is considered for transferring large number of files. Symmetric key must be kept secret and has to be transmitted to receiving end yet, that means it has to be captured by a spy to illegally decrypt the message. To establish the shared key using only symmetric key is a way difficult so the asymmetric key is recognized for sharing of key between two parties. Some examples of symmetric key include AES, DES, etc.

2) Asymmetric key encryption: Asymmetric or public key cryptography uses two key one public key for encryption of data and one private for decryption of data. It is the newer encryption as compared to symmetric key. It is computationally infeasible to figure the private key based upon public key, due to this public keys can be shared freely, allowing users for easy and suitable method for encrypting content, while private keys are kept secret The authentication claims that it's belong to the user and have not being altered or swapped by any malicious file, Due to computational complication of asymmetric encryption it is only used for small chunks of data. There are two security benefits for encryption. Asymmetric key does not allow the hacker to forge licences for others. The security services provided by asymmetric key is authenticated, confidentially and non-repudiation [18]. Symmetric key for delivering confidential, integrity and security, users should be certain that public key is authenticated, that it belongs to the user and has not been tampered or replaced by the third party. The data should be protected and kept safe. One key in the pair can be shared with everyone, that's why it's called a public key [19].

a) Confidentially*:* An individual's content is encrypted in specific public key, it can only be decrypted using specific private key, confirming that only proposed receipt can decrypt can used the data. Confidential data can only be accessed, used and copied by authorized users.

b) Integrity: It is a part of decryption process that verifies contents of original encrypted message with new decrypted match, so even a little change in the original content can cause failure to decryption.

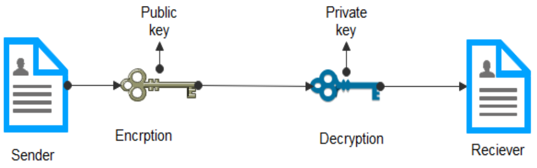

Fig. 7. Process of Cryptography [16].

V. Conclusion and Discussion

In this paper the information about the biometric data security over cloud computing is discussed by storing data on the cloud server to protect it from the criminal, hacker, etc. Cloud computing is an evolving model with the new aspects and capabilities, for maintaining the data of cloud is dominant. Blockchain technology utilizes cryptography for securing data of the user, ensuring that the transaction is done safely and storing all the secure information. The public key cryptography key is used in the blockchain to encrypt the data in the form of chunks and creating chains for holding transaction of data and afterward decrypting using private key, the secure information is stored in the cloud server to be accessed only by the user and the server.

References

[1] R. Kaur and J. Kaur, "Cloud computing security issues and its solution: A review," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 1198-1200.

[2] M. Velciu and V. Patriciu, "Methods of reducing bio-cryptographic algorithms computational complexity," 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, 2014

[3] B. Dhanalaxmi and S. Tadisetty, "Multimedia cryptography—A review," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, 2017

[4] M. Fadil and A. M. Barmawi, " M. Velciu, A. Pătrașcu and V. Patriciu, "Bio-cryptographic authentication in cloud storage sharing," 2014 IEEE 9th IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, 2014

[5] Improving bio-cryptography authentication protocol," 2015 9th International Conference on Telecommunication Systems Services and Applications (TSSA), Bandung, 2015.

[6] H. S. G. Pussewalage, J. Hu and J. Pieprzyk, "A survey: Error control methods used in bio-cryptography," 2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Xiamen, 2014

[7] L. Zhu, C. Zhang, C. Xu, X. Liu and C. Huang, "An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing," in IEEE Access, vol. 6, pp. 19025-19033, 2018.

[8] S. Luo, J. D. Seideman and S. Dietrich, "Fingerprinting Cryptographic Protocols with Key Exchange Using an Entropy Measure," 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, 2018, pp. 170-179.

[9] S. Hosseini, "Fingerprint vulnerability: A survey," 2018 4th International Conference on Web Research (ICWR), Tehran, 2018, pp. 70-77

[10] M. Sato and S. Matsuo, "Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography," 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, 2017, pp. 1-8.

[11] H. Halpin and M. Piekarska, "Introduction to Security and Privacy on the Blockchain," 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, 2017, pp. 1-3

[12] N. Kajal, N. Ikram and Prachi, "Security threats in cloud computing,"*International Conference on Computing, Communication & Automation*, Noida, 2015, pp. 691-694.

[13] R. A. R. Shaikh and M. M. Modak, "Measuring Data Security for a Cloud Computing Service," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, 2017, pp. 1-5.

[14] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat and L. Njilla, "Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack," 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Madrid, 2017, pp. 458-467.

[15] I. Sukhodolskiy and S. Zapechnikov, "A blockchain-based access control system for cloud storage," 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, 2018, pp. 1575-1578.

[16] A. Arora, A. Khanna, A. Rastogi and A. Agarwal, "Cloud security ecosystem for data security and privacy," 2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence, Noida, 2017, pp. 288-292.

[17] M. Derfouf, A. Mimouni and M. Eleuldj, "Vulnerabilities and storage security in cloud computing," 2015 International Conference on Cloud Technologies and Applications (CloudTech), Marrakech, 2015, pp. 1-5.

[18] S. Rajeswari and R. Kalaiselvi, "Survey of data and storage security in cloud computing," 2017 IEEE International Conference on Circuits and Systems (ICCS), Thiruvananthapuram, 2017, pp. 76-81.

[19] P. Tasatanattakool and C. Techapanupreeda, "Blockchain: Challenges and applications," 2018 International Conference on Information Networking (ICOIN), Chiang Mai, 2018, pp. 473-475.