Turkish Journal of Computer and Mathematics Education Vol.12 No.14 (2021), 5254-5270
Research Article

Cloud methods electronic health services (EHS), for improving cyber security and privacy data, suggest solutions for unauthorized access issue

Raed Al-hamarneh

Computer and Information System Department, University of Almaarefa, Riyadh,

Kingdom of Saudi Arabia, Email: al-hamarneh:rhamarneh[at]mcst.edu.sa

Abstract

in 2020 was certainly not a traditional year. The pandemic make huge pressures on cyber security, IOT, leaders and businesses were forced to rapidly accelerate their digital transformation plans and massively expand their remote working capabilities. Cyber actors seized the opportunities created by the pandemic and exploited vulnerabilities in security defenses to gain access to business networks and sensitive data. In 2020, phishing and ransomware attacks increased, as did web application attacks, according to the recently published Verizon 2021 Data Breach Investigations Report. The report provides insights into the tactics, techniques and procedures used by nation state actors and cybercriminal groups and how these changed during the pandemic. To improve the cloud security, I used very important methods, in my proposal system very secure devices that contribute to reduce or avoid for illegal access cloud computing , all medical services ,must be secure (store , transfer).

In this paper, we propose new EHS sharing framework that combines modern technology and the centralized system on a cloud platform. Particularly, we design atrustworthy access control mechanism using smart contracts to achieve secure EHRs sharing among differentpatients and medical providers

Keywords: cyber security, Data Breach Investigations,vulnerabilities,sharing framework

1. Introduction

At arecent time when health institutions are mobilizing all their possible efforts to confront the emerging corona virus, the World Health Organization and a number of hospitals and medical institutions have been hacked and cyber-attacks in search of information related to treatments, tests and vaccines for the virus, somost of e-health services still under attack byRansomware(Lab, 2021).

Cloud computing support a new technology to all specific filed tomake a virtual IT department via the Internet [1, 2]. The cloud computing offers different virtual services like traditional IT department, such as storage, stream server and database server. The cloud provides a cost-effective model through pay-per-use that allows each individual or businesses in healthcare start a cloud-based service with minimum investment(Rodrigues, 2009)(Singhal, 2015). However, the cloud computing has several major cybersecurity issues for an eHealth system which are discussed as follows. One of the main objectives that is offered from this IT technology for the companies is reduced time and costs. Cloud computing is supporting companies and organizations to use shared storage and computing resources.

A blockchain is a public database of records distributed over multiple peers on a network. (P. Ora, 2015).The most important property of immutability allows it to work as a secure database. It is not only confined to 'Bitcoin' anymore but has deeply rooted itself in other fields. One of such fields is e-health systems. The high priority of data associated with this field demands a professional security method. Blockchains provide this required solution. They can be used in almost every aspect of e-health systems from patient education to fighting counterfeit drugs (Mettler, 2016)

Patients now can inquire their personal health data at home based on electronic devices (such as smartphones and wearable sensors) and share on cloud environments where application can access instantly to access medical records and provide timely medical supports. This smart e-health service access healthcare providers remotely monitor patients and offer ambulatory care at home, which not only facilitates healthcare delivery but also brings economic benefits to patients. Further, the availability of complete EHRs on clouds also helps healthcare providers track patient health and offers proper medical services during diagnosis and treatment processes (Madisetti, 2013)

2. Related work

Many studies have been conducted for improving e-health security by using cloud computing, There have been several traditional solutions to deal with the problem of secure EHSs sharing on cloud environments for For Unauthorized Access,Clemens Scott Kruse and other provide amazing summary, focusing about most frequently security measures and techniques are three themes: administrative, physical, and technical safeguards. The information contained within electronic health records has prompted the need for advanced security techniques that are able to put these worries at ease. It is imperative for security techniques to cover the vast threats that are present across the three pillars of healthcare. **(Clemens Scott Kruse, 2017)**

K.S.Suresh and Prof K.V.Prasad provide Cloud Computing is the use of activity of using Computer hardware and software. Cloud Computing is support IT Services that are provided to a customer over a network and all services . It is often "as a service" over the Internet, typically in the form of infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service**(M.Tech2012 ،)**

Amazing Author Livia Maria write about many advantages of this type of technology, the usage of equipment managed by a cloud service provider to process, transmit and store data may cause concern about maintaining an adequate level of security, so that important information for users is protected. According to a study carried out by CSA - Cloud Security Alliance, the customers main concern of regarding the migration to a public cloud platform is the security of the data along with the leakage risk and the regulatory compliance (Figure 1)**(BRUMĂ, 2020)**

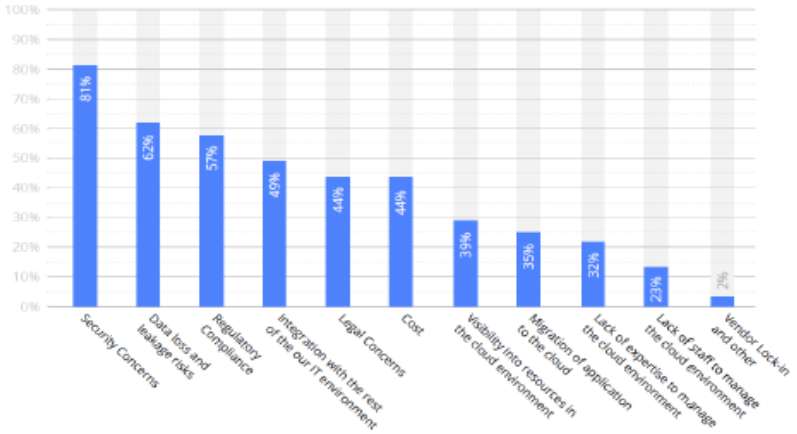

Figure1: The main reasons for concern of cloud users [12]

One of the most important websites that discuss the topic of cloud computing, which discusses security issues and one that you talk about data theft, the main issue is illegal access and view our customer issues, and provide professional solution to many issues.**(Anon., 2021)**

Artificial intelligence has become one of the most important elements in electronic health services, especially in electronic security issues, and Punithavathi P. emphasis The growing demand for biometrics solutions in digital healthcare system is mainly driven by the need to combat fraud, along with an initiative to preserve privacy of the patient besides with healthcare safety, especially in Biometrics **(Punithavathi P. (VIT Chennai, 17)**

In one of most challenges of cloud security studies,used we have used the Rijndael Encryption Algorithm along with EAP-CHAP, in Figure 2, the methodology The steps of the methodology , the concluding write"Even if some intruder (Unauthorized user) gets access of the data accidentally or intentionally, he will not be able to decrypt it. Also, it is proposed that encryption must be done by the user to provide better security. Henceforth, security is provided using Rijndael Algorithm" (**Singh, 2013)**

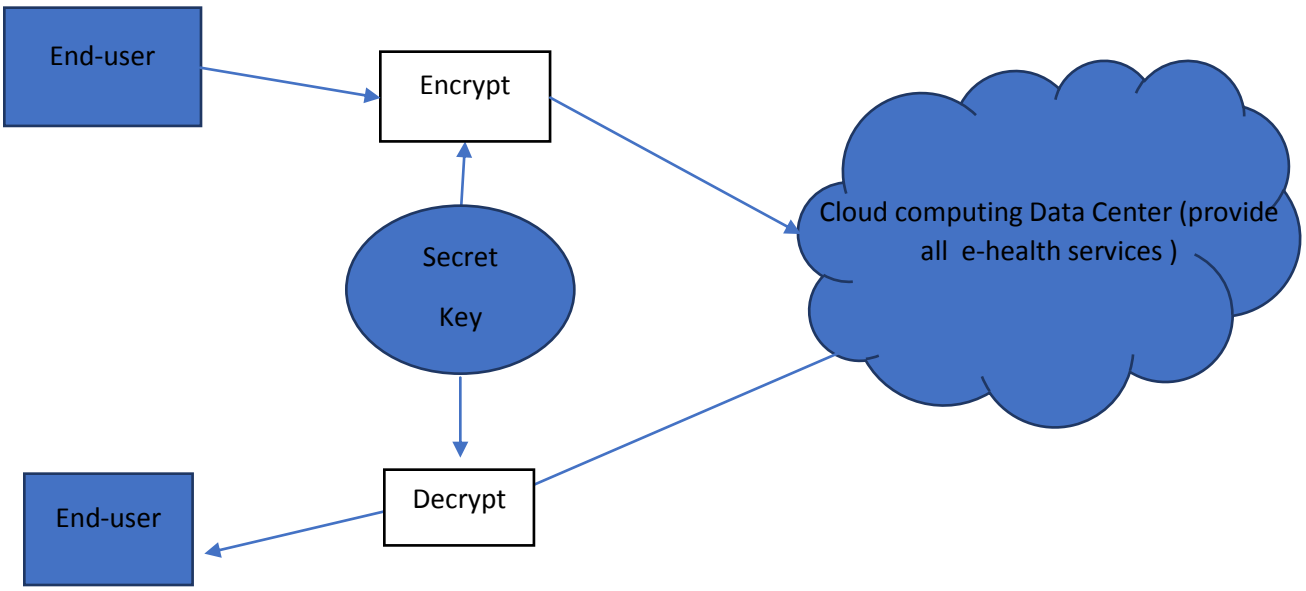

Figure2:Methodologyof the Rijndael Encryption Algorithm along with EAP-CHAP

In papertittle" Research issues for privacy and security of electronic health services", evaluate state-of-the-art electronic health system research based on their architecture, as well as services including all services (access control, emergency access, sharing, searching, and anonymity) methods by considering their cryptographic approaches. our key contribution is to present state-of-the-art approaches regarding security, privacy, and integrity aspects of EHS by considering the components and challenges of e-health services. systematically evaluated the studies with a method-based approach, and provided a comprehensive survey of cryptographic approaches of EHS. Our major contribution is to categorize state-of-the-art EHS studies into different aspects **(other, n.d.)**

3. New ProposalArchitecture in e-health

I will provide new proposed to enhance security in cloud computing, using money of algothims and techniques I will explain in details in my paper that will focus in all modern techniques.

I present architectures used in EHS, which are cloud . centralized architecture because privacy and security research issues are prevalentin decentralized settings and the techniques for providing privacy and security can be easily applied to a centralized setting.

In Figure3 see e-heath services , all transaction between all supervision and cloud commutating must encrypted , the main issues I will focus in my paper talk about untheorized person , how to deal , I think is the elephant in your room, now e-health services for every organization , used web portal and mobile application , if any illegal persons

will theft all data , destroy , so I suggest amazing environment technology will reduced for unnotarized person , hacker.

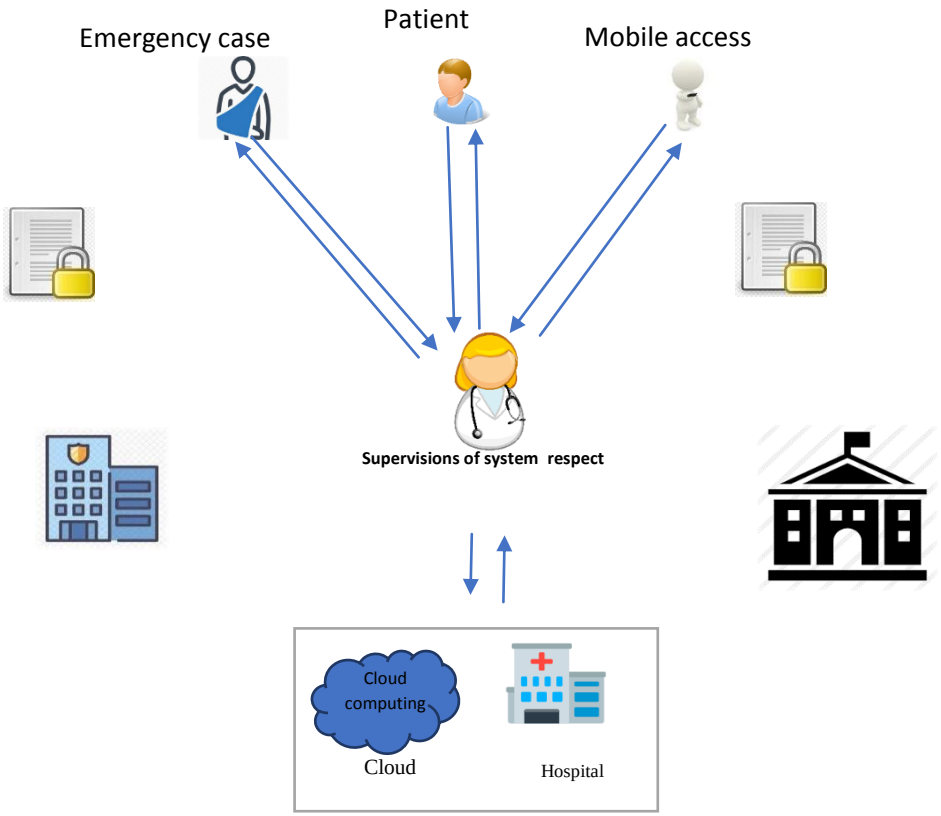

Figure3:overview of cloudarchitecture

4. OVERVIEW OF THE PROPOSED SCHEME

In our approach, users are health-care practitioners, and patients and medical centers represent data owners who store encrypted health-care records in the cloud, to perform most of the computation-intensive tasks including authentication and fine-grained data access control. The architecture minimizes the computational overhead on the data owner's side as wellas the time that data owners are required to be available online ,I worked with some algothims, and technology in figure 4 see the new connection and how to make it with out hacking that :

I. Neural Network algorithms
II. Hard disk encryption
III. Biometrics security technology

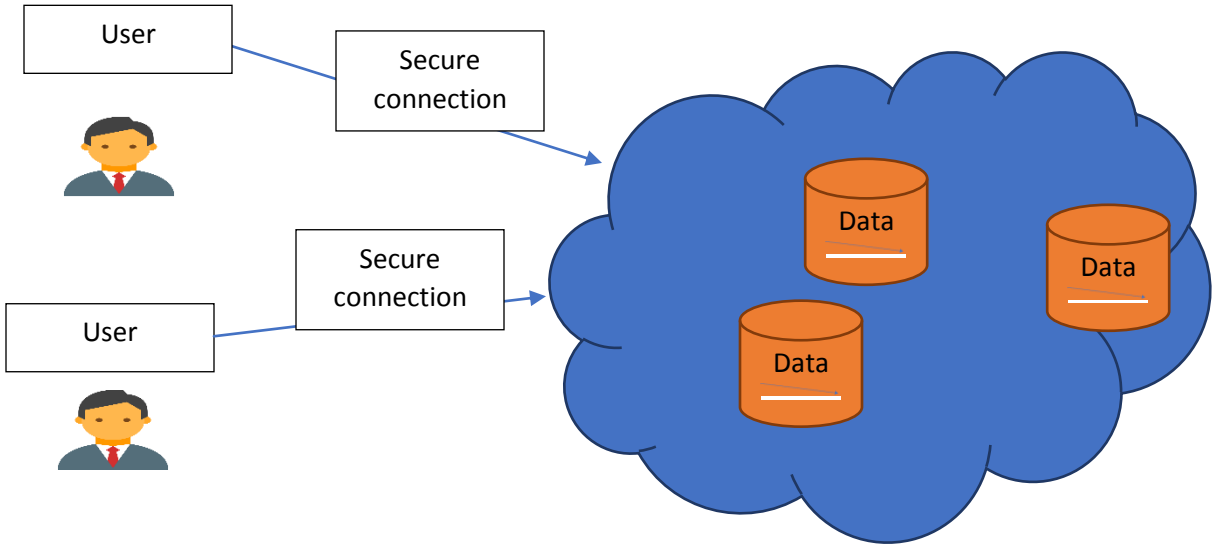

Figure4: Deep my e-health connectionservices security in cloud

I. Neural network encryption

Neural networks, also known as artificial neural networks (ANNs) or simulated neural networks (SNNs), are a subset of machine learning and are at the heart of deep learning algorithms. Their name and structure are inspired by the human brain, mimicking the way that biological neurons signal to one another.

Artificial neural networks (ANNs) are comprised of a node layer, containing an input layer, one or more hidden layers, and an output layer. Each node, or artificial neuron, connects to another and has an associated weight and threshold. If the output of any individual node is above the specified threshold value, that node is activated, sending data to the next layer of the network. Otherwise, no data is passed along to the next layer of the network.

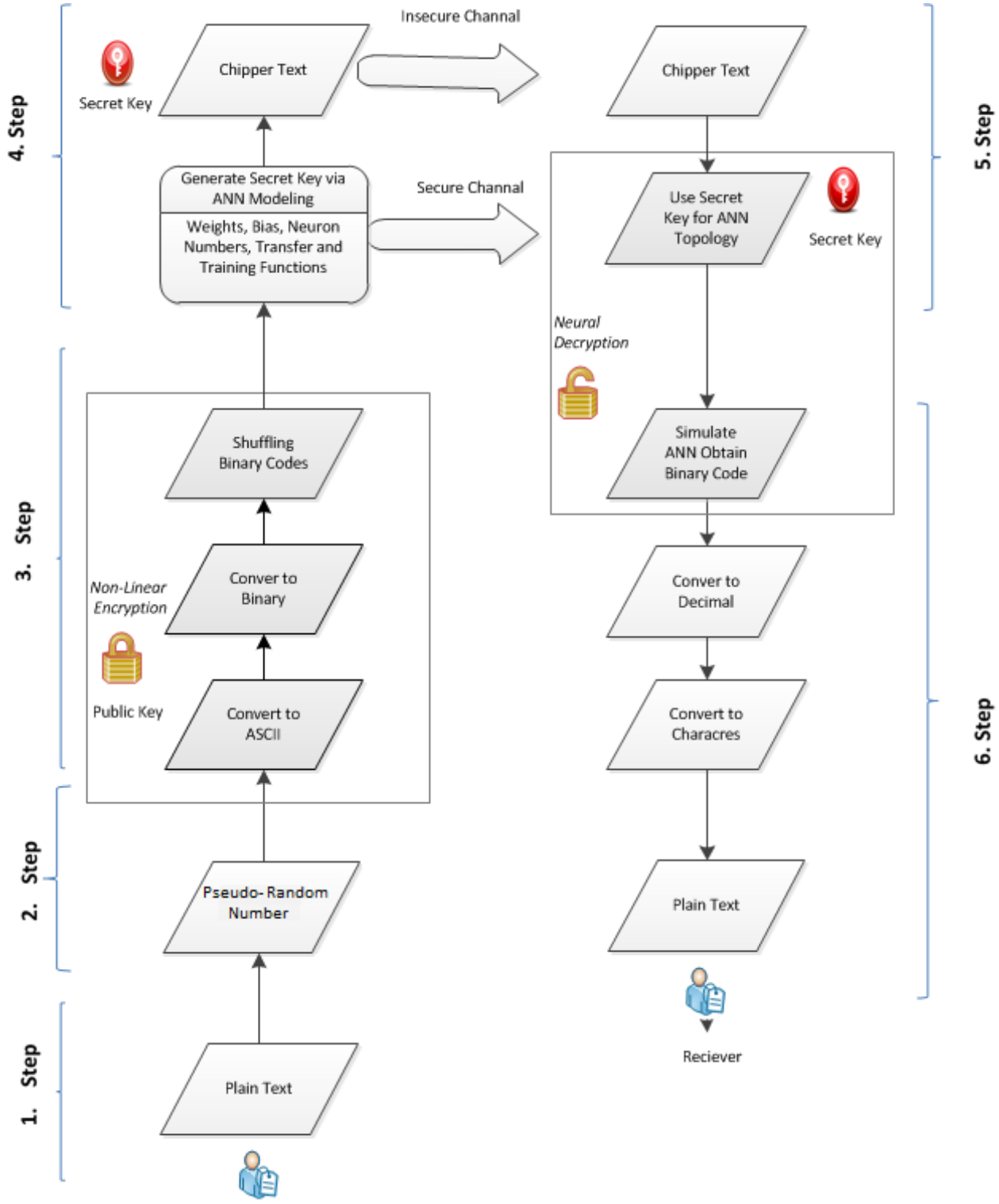

Figure5: secure channel between users and clouded **computing (Anon., April 14, 2014)**

The human body renovates itself and generates a variety of reactions against theincidents that occur during physical, biological or chemical changes, in order tobecome used to them. The structures of this system, which complement with eachother, have inspired a great number of scientists. Variations occurring in our environment are detected by neurons in our bodies, which are then transmitted toour brains. The brain works as a decision-maker, alerting sub-systems to producethe optimum reaction

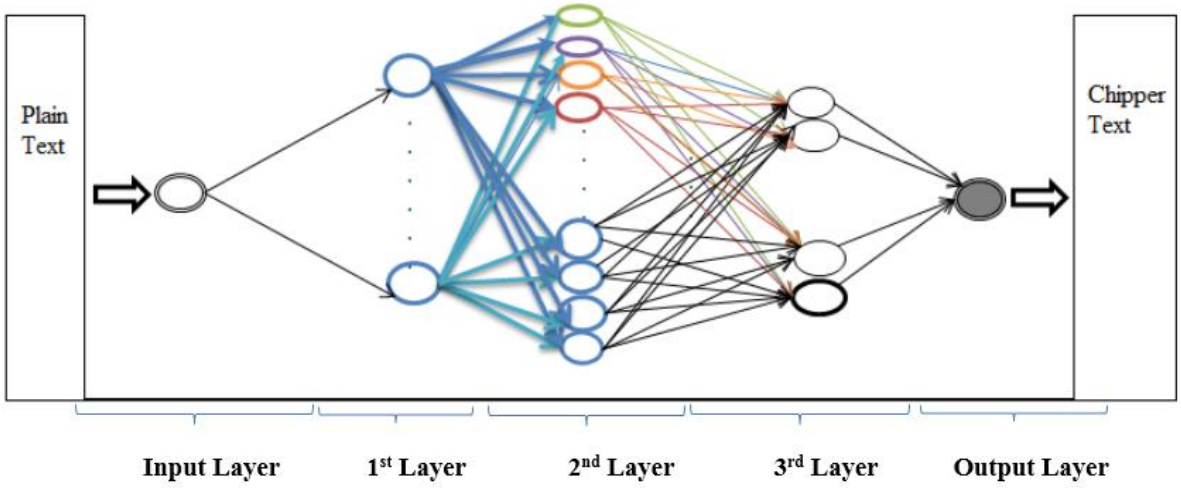

Figure6: Designed topological neural network.(Anon., April 14, 2014)

In Figure 6: Architecture of a simple neural network described by the input, output, and a hidden layer in between. Information flows through all layers, starting from the input layer to the output layer. Herein, every neuron receives information from all neurons of the previous layer (in literature called a fully connected layer). *e connections θ between the processing blocks are the parameters that have to be adjusted in accordance with data and the formulated problem. Each processing block performs a transformation (herein a weighted sum of the input parameters) and the result is passed to an activation function f that will be used to add nonlinear properties in the network. Activation functions are usually selected from a set of limited functions with certain mathematical properties. Nonlinearity is needed to allow for a complex arbitrary functional mapping between input and the output data **(Vizitiu, 2020)**

II. Hard disk encryption

Encryption of data at rest can be divided in to following four categories:

1. File level encryption: In file level encryption, data is encrypted onfile by file basis.
2. Folder level encryption: In folder level encryption, data isencrypted on folder by folder basis.
3. Partition level encryption: In partition level encryption, for dataencryption a partition is created. Any data copied in that partitionwill be encrypted automatically without any action.
4. Disk level encryption: In disk level encryption, whole disk isencrypted including all files, folders, operating system and in orderto boot, an authentication mechanism is required. It is implementedfully on the fly i-e before written on the disk; data is encrypted andonly decrypted before use.

Basically, encryption refers to the process of encoding data. In disk encryption, this means that information on your computer's hard drive is converted from plaintext to ciphertext, which makes the original information unreadable. Hard drive encryption uses a specific algorithm, or cipher, to convert a physical disk or logical volume into

anunreadable format that cannot be unlocked by anyone without the secret key or password that was used to encryptthe drive. This prevents unauthorized people or hackers from accessing the information. **(Pekkarinen, 3rd of November, 2020)**

There are two main computer encryption types: full disk encryption and file-level encryption.

1. Full Disk Encryption (FDE) or whole disk encryption protects the entire all files on the drive against unauthorized access.
2. In contrast to FDE, File-Level Encryption (FLE) is an encryption method, which takes place on the file system level, enabling the encryption of data in individual files and directories.

III. BitLocker Drive Encryption:

The method used in user,individual Encrypted Hard Drive uses the rapid encryption that is provided by BitLocker Drive Encryption to enhance data security and management.

By offloading the cryptographic operations to hardware, Encrypted Hard Drives increase BitLocker performance and reduce CPU usage and power consumption. Because Encrypted Hard Drives encrypt data quickly, enterprise devices can expand BitLocker deployment with minimal impact on productivity.

Encrypted Hard Drives are a new class of hard drives that are self-encrypting at a hardware level and allow for full disk hardware encryption. You can install Windows to Encrypted Hard Drives without additional modification beginning with Windows and Windows Server

Encrypted Hard Drives provide:

1-Better performance: Encryption hardware, integrated into the drive controller, allows the drive to operate at full data rate with no performance degradation.

2-Strong security based in hardware: Encryption is always "on" and the keys for encryption never leave the hard drive. User authentication is performed by the drive before it will unlock, independently of the operating system

3-Ease of use: Encryption is transparent to the user, and the user doesn't need to enable it. Encrypted Hard Drives are easily erased using on-board encryption key; there is no need to re-encrypt data on the drive.

4-Lower cost of ownership: There is no need for new infrastructure to manage encryption keys, since BitLocker leverages your existing infrastructure to store recovery information. Your device operates more efficiently because processor cycles do not need to be used for the encryption process.

iv. Biometrics security

1. Authentication

encryption system is only as good as the authentication system that allows users to access their computers, so ensure any system you consider offers a range of two factor authentication methods allow biometrics to be used.

Biometrics is one of the most important factor that using of employee access to the cloud viacomputer, one of most advantage which if forgot password, you can work s works with your data, any case we will deal with the collection of biometrics in detail.

Examples of Biometric Security

- Voice Recognition
- Fingerprint Scanning
- Facial Recognition
- Iris Recognition
- Heart-Rate Sensors

2. Algothims1 my proposal System :

IV. Between user and cloud computation via (. mobile, laptop)

neural network encryption

1- Collect biometric sample from user in client side
2- The user put his name and password.
3- The server cloud generate OTP, The client put the OTP, can access the cloud computing
4- The user put OTP and neural network start encryption between user and cloud computing
5- The Data started Encrypted, DATAENRNur(DATA,OTP)
6- Encrypted, DECDATAENRNur(DECData,OTP)
7- Using Hard disk encryption (locked hard disk) with any illegal access with some criteria (
    - Three-time OTP wrong
    - Access three-time error (username or password)
    - Not recognized IP(Pool IP) must provided by
8- To unlockedhard diskusing Biometrics security
    a. Fingerprint Scanningusing minutiae extraction algorithm.
    b. Iris Recognition using minutiae extraction algorithm
9- END

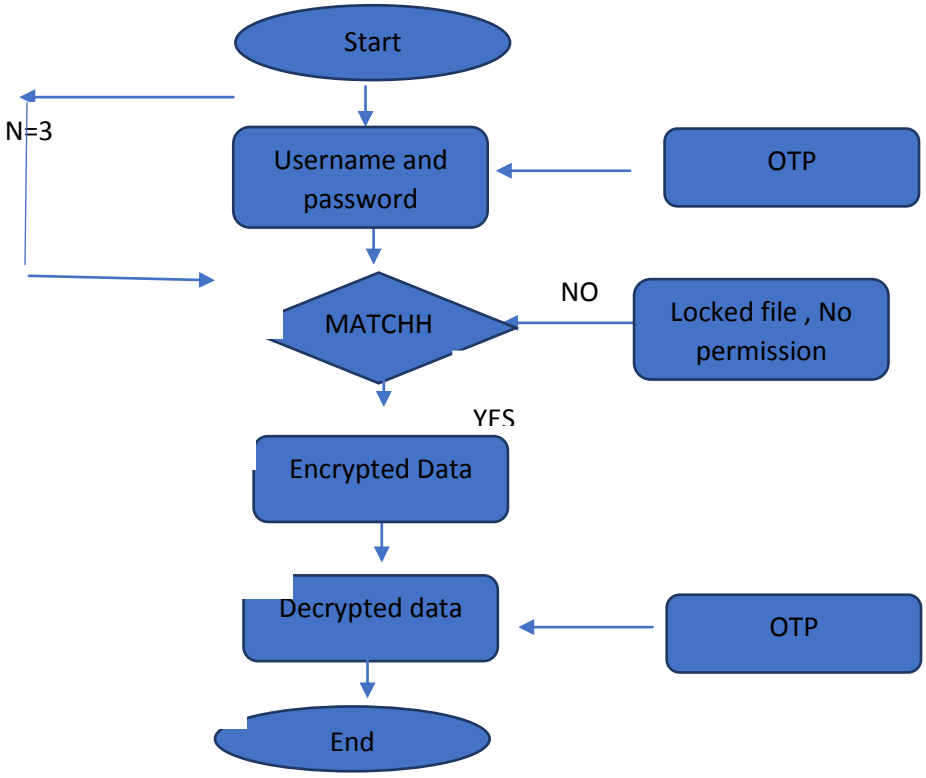

Figure7: Proposed architectureof encryption system with OTP

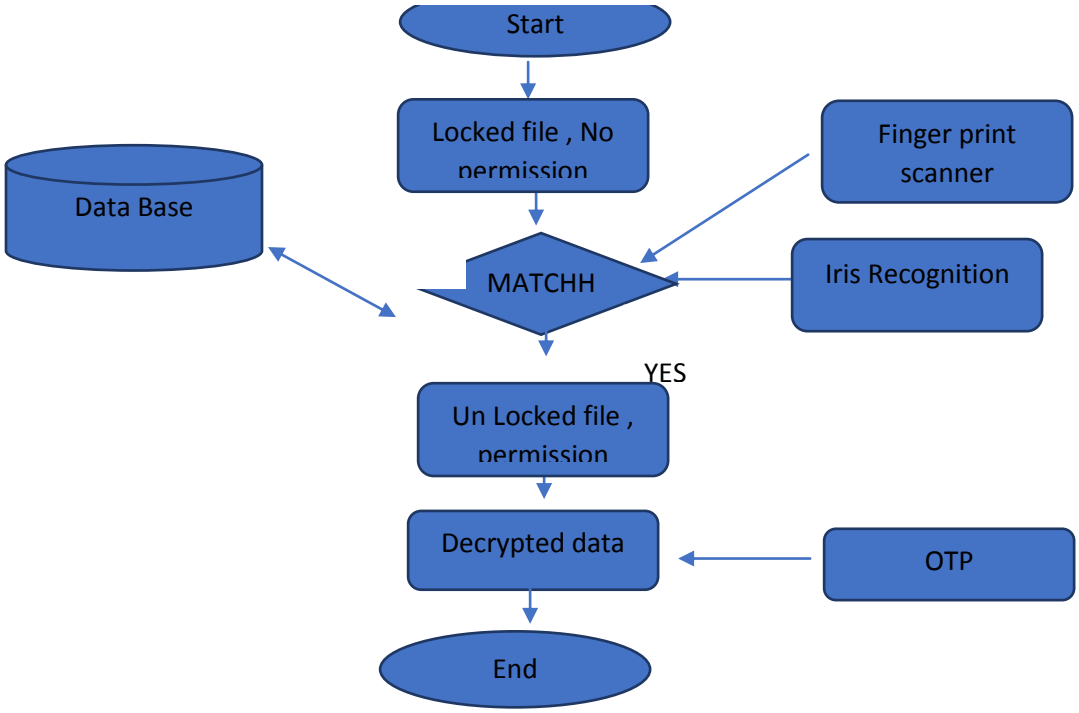

Figure8: Proposed architecture of encryption using biometrics

Using procedures given in algorithm 1, the workingflowchart are shown in Figure 7, First the user put username and password to open his file , received OTP from servicer as SMS in his /here mobile can start encrypted to transfer , if the user have try three times user name or password or OTP wrong .

In Figure 8 ,describe how to solve illegal access , hacker and cracker , used not correct OTP,many time username and password , must locked file using hard disk encryptions , to unlocked file By using the minutiae extraction algorithm advantages will be extracted from the biometric sample which is the template. One another template is also stored in the cloud database. The user entered the template by utilizing fingerprints and iris eyes Its time to verify the template using the stored template in the cloud database. After verifying ,it will unlocked the file the client access and send OTP for user to send encrypted data to cloud And encrypt the user data using the advanced encryption algorithm and send the encrypted data to the client which is called ED(Encrypted Data). Most important thing is that the cloud authentication server also sends the one time password using the HTTP gateway to the user. If biometrics failed(emergency case) all hard disk encrypted , send SMS to Admin " attempt to cloud not access ".

V. RESULTS

This section describes the performance evaluation of the proposedapproach. The assessment of other methods with theproposed technique is likewise proven. As the minutiae extraction Algorithmdiminishes an opportunity to separate the detailsfromthe biometric test, we pick the algorithmto process the biometrictest in our strategy OTP includeacheck factor in verification with the goal that the clientneeds to give various messages to confirm each time. By alongthese lines, the application themselves can acquire higher securityensure than those utilized static secret word innovation. Atlast, we figure the procedure execution time and afterward contrastedand different existing technique and results are recordedin the table.

I. Simulation environment

In my proposal Iused my laptop The usage is done in an indistinguishable PC with an ntel(R) Core(TM) i5 CPU M 460 2.70 GHz processor and 8GB RAM, 6.00 GB (5.68 GB usable)

Hardware a will two biometric devices:

1. Digital Persona U-are-u 4500 Fingerprint Reader: The U.are.U 4500 Fingerprint Reader is an optical USB fingerprint reader and perfect for individual desktop users, as well as multiple users in shared environments. Its compact design conserves desk space in enterprises, and its professional, modern appearance looks elegant in point-of-scale environments.
2. CMITECH EMX-30: The EMX-30 is a fully hands-free, dual iris imager intended for desktop, countertop and kiosk enrollment and authentication applications. This lightweight and compact system operates at a stand-off distance range of 32 to 35 cm. The EMX-30 features a simple and intuitive user interface, making it easy to use and integrate, even for subjects with minimal acclimation. The EMX-30 provides exclusive subject positioning distance indicators, so that the subject can quickly and reliably place his or her eyes within the capture zone. Thanks to its unique distance calculation capability, subjects no longer need to guess at or hunt for correct eye placement. LED's located within the mirror's display easily guide the subjects into the correct position: a blue light indicates too far away, red too close, and green indicates the correct distance.

This is the time to integrate hardware and software for this architecture. At first, open the fingerprint verification software and set the serial port. we can do enroll and detect the fingerprint. After enrollment is complete, we can do register for any employee who work with cloud . so we can do iris in . CMITECH EMX-30 Device . After completion of the registration process. By opening the verification software, we can find our ID. Besides the encryption–decryption software also works. It takes all information from the database, and via email we get the OTP key to encrypt the information. After encryption, using the OTP we can complete the decryption of our data.

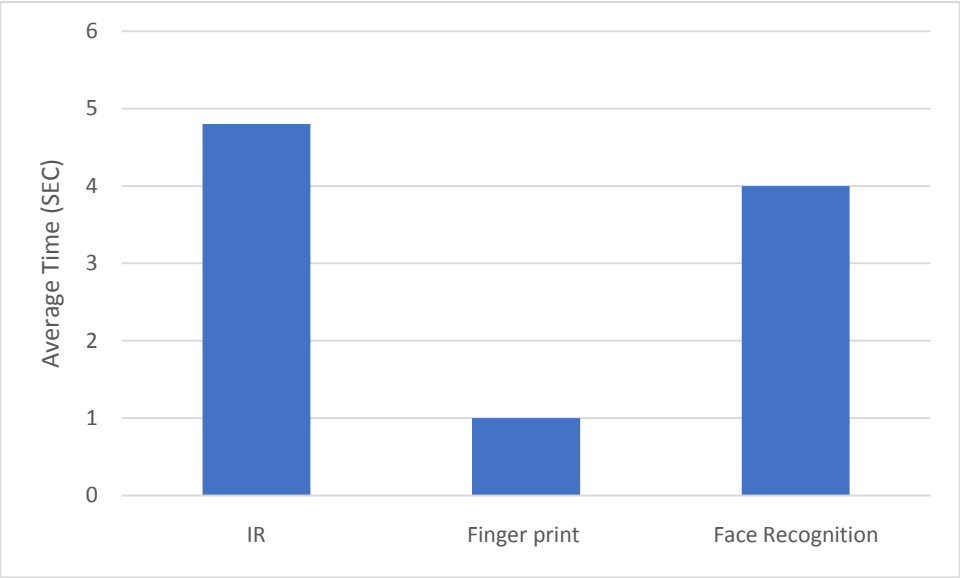

Figure 9. Comparison of the proposed hybrid technique's average time with various biometric techniques average time

I. Hard disk encryption analysis:

BitLocker (Windows): Setup may vary from one version/edition to another, but for example, on Windows 7 Ultimate or Enterprise editions, BitLocker can be turned on by entering the Control Panel application, choosing Security, clicking on BitLocker Drive Encryption, choose a drive to encrypt and follow instructions to enable drive encryption

For more information on Full Disk encryption feature in BigFix MCM, see Full Disk Encryption.

Workflow to configure and deploy Full Disk Encryption

1. Set up the BES Server Plugin Service (Fixlet 708 in BES Support)
2. Configure Recovery Key Escrow
3. Create Disk Encryption policy
4. Deploy FDE Policy

Using the properties from the "Full Disk Encryption Status" analysis, you can enable columns that allow filtering to look for devices that are not encrypted, missing recovery key, and so on

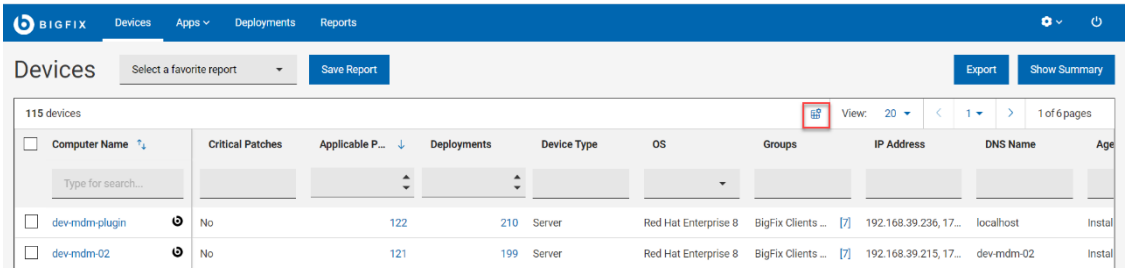

Figure 9: Report of encrypted hard disk

To include the Full Disk Encryption specific device properties in the device data grid:

1. From the device list, click manage column icon.
2. In the Manage columns window, search by string in the Property name field or in the Analysis column, select Full Disk Encryption.

Neural network encryption

Neural-based pseudo-random numbers and traditional pseudo-random numbers were explained and tested with NIST randomness tests. These tests are believed to be useful in detecting deviations of a binary sequence from random-ness. The results of the randomness tests are shown in Tab. I and Tab. II. In Tab. I, the randomness test results and the details of NN-based PRNGs are ex-plained. The proposed NN-based PRNG successfully passed the test, as described in Tab. I. In Tab. II, results for the randomness of numbers generated by a mod- I filed subtraction with borrow random number generator are shown. Frequency test, runs test, longest run of ones in a block test and cumulative sum test were all failed. The other tests were passed Comments on the passed test are described in Tab. II and the failure results are explained below. The frequency test is the first randomness testing step. It defines whether zero and one bits appear in the tested sequence with approximately the same probability. Clearly, classic RNGs could not pass the basic randomness test. Indeed, there is no need to analyze other tests when the frequency test is failed Furthermore, 0.000233 p value (>0.01) describes the correlation between zeros and ones in the sequence. However, pseudo-random number sequences must not be in correlation with each other. Theruns test defines whether or not transitions between zeros and ones in the sequenceappear as frequently as expected in a random sequence. 0.000212 p value (> 0.01)

indicates that runs in a random sequence generated using a modified subtract withborrow random umber generator are too slow or too fast, suggesting a non-randomwalk. The longest run of ones in a block test determines whether or not the lengthof the longest run of ones in a block is consistent with the length expected froma random sequence.

A 0.000368 p value (> 0.01) suggests that the cumulative sum in a random sequence generated by a modified subtract with borrow random num-ber generator is too large or too small, indicating a non-random walk. Tabs. I and Tab. II show that the neural-based pseudo-random generator is much more successful than the modified subtract with borrow algorithm. It can, therefore, be said that the neural network can be used to improve randomness

Tests	p Value	Result	Comments
Frequency Test	0.14986	Success	0 and 1 bits appear in the sequence with approximately the same probability.
Block Frequency Test	0.911733	Success	0 and 1 bits appear in the blocks of sequence with approximately the same probability.
Runs Test	0.85160	Success	Transitions between 0 and 1 bits in the sequence appear as often as expected from a random sequence.
Longest Run of Ones in a Block Test	0.093350	Success	The length of the longest run of 1 bits in a block is consistent with the length expected from a random sequence.
Cumulative Sum Test	0.911733	Success	The cumulative sum of the partial sequences consist of the tested sequence is not too large or too small relative to the expected behavior of that cumulative sum for random sequences.
Discrete Fourier Test	0.646355	Success	The number of peaks exceeding the 95% threshold is not significantly different than 5%.
Rank Test	0.741908	Success	The deviation of the rank distribution of the sequence can be ignored.

TABLI:tRandomness testing results of number generated by ANN based pseudo-random number generator

Tests	p	Result	Comments
Frequency Test	0.00023	Failure	
Blok Frequency Test	0.234600	Success	0 and 1 bits appear in the blocks of sequence with approximately the same probability.
Runs Test	0.00021	Failure	
Longest Run of Ones in a Block Test	0.000001	Failure	
Cumulative Sum Test	0.000368	Failure	
Discrete Fourier Test	0.408863	Success	The number of peaks exceeding the 95% threshold is not significantly
Rank Test	0.741908	Success	The deviation of the rank distribute-

Tab. II Randomness testing results of numbers generated by modified subtract

with Barrow random number generator

Discussion and conclusion

In my proposal: It was found that even after considering the benefits of cloud computing, the disadvantages cannot be ignored. The major issue of the shift in the healthcare industry to the cloud computing system is that they experienced great exposure to the outside environment giving rise to security challenges and security threats The information stored on clouds can be accessed by unauthorized users by hacking the servers. It was challenging for both the users and the cloud computing service providers to protect data privacy. Algorithms and techniques(Hard disk encryption, Neural network encryption, Biometrics security) were used and proposed for securing the data and overcoming these obstacles. One of the most important methods usedClearly, deploying Biometric services in cloud environment is solution for the problems of scalability and time as well as access. But it will take a time to prove its acceptance and implementation. Few of the solutions are available in the market nowadays provided by smart devices ,Encryption of hard is the art of preserving confidentiality of digital information. It is considered to be one of the most ideal solutions for providing data confidentiality and safety of computer hard disk.

References

Abdulghani, H., Nijdam, N., Collen, A. & Konstantas, D., 2019. A Study on Security and Privacy Guidelines, Countermeasures. In: *Threats: IoT Data at Rest Perspective.* s.l.:s.n., pp. 11, 774.

Anon., 2021. *cloud Computing Security Issues.* [Online]
Available at: One of the most important websites that discuss the topic of cloud computing, which discusses security problems and one that you talk about data theft, the main issue is illegal access
[Accessed 6 19 2021].

Anon., April 14, 2014. NEURAL NETWORK BASED. pp. 177-192.

BRUMĂ, L. M., 2020. Data Security Methods in Cloud Computing. *Informatica Economică,* Volume 24, p. 48.

Clemens Scott Kruse, c. a. B. S. H. V. a. A. N., 2017 . Security Techniques for the Electronic Health Records. *Journal of Medical Systems,* p. 41(8): 127.

Lab, K., 2021. *Ransomware – definition, prevention and removal.* [Online]
Available at: https://www.kaspersky.com/resource-center/threats/ransomware
[Accessed 06 11 2021].

M. Hölbl, M. K. A. K. a. L. N. Z., 2018. review of the use of blockchain in healthcare. *A systematic,* Volume 10, p. 470.

M.Tech, K., 2012. *Security Issues and Security Algorithms in Cloud Computing,* s.l.: International Journal of Advanced Research in.

Madisetti, A. B. a. V. K., 2013. A cloud-based approach for interoperable electronic health records (EHRs). *IEEE J. Biomed. Health Inform.,* Volume 17, p. 894–906.

Mettler, 6. .. M., 2016. *Blockchain technology in healthcare: the revolution starts here.* Munich, Germany, s.n., pp. 1-3.

other, B. Y. a., n.d. Research issues for privacy and security of electronic health services. *Future Generation Computer Systems,* Volume 68, pp. 1-13.

P. Ora, P. R. P., 2015. *Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography*. india, s.n., pp. 1-6.

Pekkarinen, L., 3rd of November, 2020. Hard Drive and Full Disk Encryption: What, Why, and How?. *Miradore.*

Punithavathi P. (VIT Chennai, I. a. G. S. (. C. I., 17. Digital Healthcare Security Issues: Is There a Solution in Biometrics?. *IGI Global,* p. 2019.

Rodrigues, 2009. *Health Information Systems: Concepts, Methodologies, Tools, and Applications.* s.l.:IGI Global.

Singhal, M. B. a. M., 2015. The Role of Cloud Computing Architecture in Big Data. *Springer,* 8(Information Granularity, Big Data, and Computational Intelligence), pp. 275-295 ,Chapter 13.

Singh, S. S. &. J., 2013 . Cloud Data Security using Authentication and Encryption. *Global Journal of Computer Science and Technology*, 13(3).

Vizitiu, A., 2020. Applying Deep Neural Networks over Homomorphic Encrypted. *Hindawi*, p. 26.

WEBROOT, n.d. *What is Social Engineering?*. [Online]
Available at: https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering
[Accessed 06 13 2021].