ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.3

Implementation of Biometric Individual Identity in Healthcare and Fingerprint Recognition

Arulraj[1], M.Nithya[2], A.Parveen[3]
Assistant Professor[1], BE Student[2, 3]
Department of CSE
Dhaanish Ahmed College of Engineering, India

Abstract:
In the day today scenario each individual's biometric patterns such as(Iris scan, Finger Prints Impression)were feed to the Aadhar database and biometric characteristics is considered to be unique for every individuals. Suppose a person meet with an accident somewhere and he/she seemed to be death or is in unconscious state, it is highly difficult to trace the individual identity of the person who had meet with the accident and it is highly time consuming .Thus to eradicate this problem here is a best solution, that is each and every government and private hospitals whom were licensed by the state and central government and the government and private emergency free ambulance service to provide a Biometric Authentication Device(BMAD)that is connected with the Centralized Aadhar Database server by means of common website through web services. Through BMAD individuals biometric patterns were feed into the common website, which is connected with Centralized Aadhar database server. The main objective of the idea proposed here is to provide automated identity in health care centres for each and every individuals dwelling in the globe by matching the individual's biometric patterns with the biometric patterns stored in the existing Centralized Aadhar database server by means of Internet services and to provide emergency alerts (SMS services or Phone call) to the family of the concerned individual.

Keywords: component; formatting; style; styling; insert (key words)

I. INTRODUCTION

The main objective of the idea proposed is to provide automated identity in health care centers for every individuals dwelling in the globe by matching the individual's biometric pattern stored in the existing Centralized Aadhar database server by means of Internet services and to provide emergency alerts (SMS services or Phone call) to the family of the concerned individual.

Biometrics Authentication Technology:
Biometrics was automated methods of identifying a individual or verifying the physiological or behavioral characteristics. Biometrics is real-time mechanism that can be combined with other mechanism to make more securitized, easy usage of verification solutions identifying individuals. Presently the various existing biometric characteristics were fingerprint scan, facial scan, retinal scan, iris Scan, vein pattern scan, digital signatures, keystroke dynamics, voice scan, hand and finger geometry and so on.

EASE OF USE

A: Our contributions and motivation

We keep multifaceted contributions in this proposed article

1) We present a new robust, secured remote authentication scheme that uses extended chaotic map, user biometrics and user smart card simultaneously.
2) We introduce an efficient mechanism for revocation of a lost user smart card.
3) We present an in-depth performance comparison with the existing related schemes that shows the efficiency of the proposed scheme.
4) We provide a detailed informal security analysis that explains why the proposed scheme is robust and secured..
5) Through the formal security verification using BAN logic, we prove that the proposed scheme achieves unconditional security.

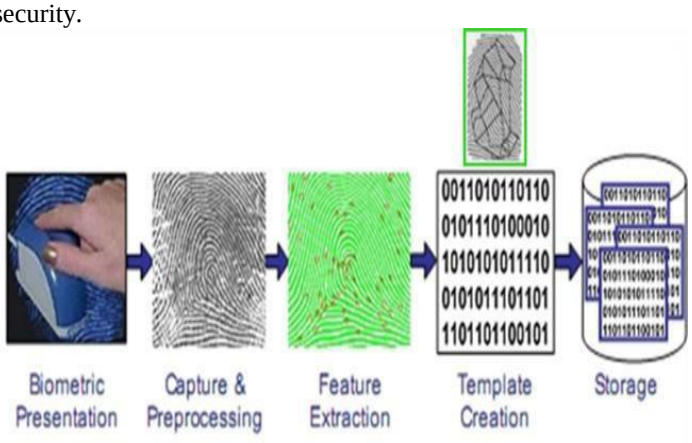


Figure.1. storing biometric character tics into database

Biometric technology is used in wider area in various applications like organizations and E-Governance services, National Security, Airports, Banks, offices. Later implemented in ATM machines, voting Machines, net banking and in Attendance monitoring Systems. Biometric technology is used in wider area in various applications like organizations and E-Governance services, National Security, Airports, Banks, offices. Latently implemented in ATM machines, voting Machines, net banking and in Attendance monitoring Systems.

Benefits of Biometric technology:

Biometric technology has various benefits in uniqueness, global acceptance, universality, static, measurable, user friendly, accurate and comfortable to use.

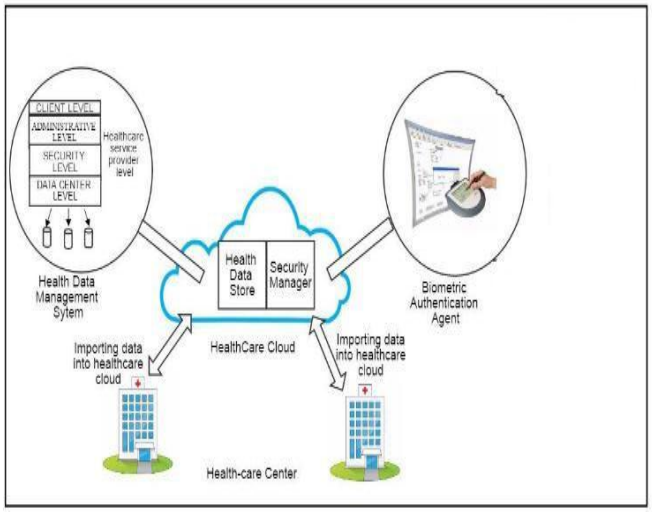


Figure.2.Healthcarecloudand application

Unique Identification (UID): The unique identification (UID) is a mission mode that provides identification for citizens residing in the country and it is used primarily for delivering welfare services to the citizens effectively. It also act as an effective mechanism to monitor enormous schemes and programs of the government. Authentication framework contains UIDAI and its supporting organizations such as AUAs (Aadhaar User Agencies) & KUAs (e-KYC User Agencies), whom were the service providers or government elements who provides Aadhaar authentication as part of their delivery of service and ASAs (Aadhaar Service Agencies) & KSAs (e-KYC Service Agencies) those who provides AUAs & KUAs securitized connectivity of network to UIDAI's CIDR. The Unique Identification Authority of India (UIDAI) is responsible to lay plans and policies to real time existence of UID scheme, to govern and maintaining the UID database and to make updates and to maintain the database.

II. PROBLEM DESCRIPTION

A. HealthCare Cloud

Let HC denote the health care cloud Hc={S, P, D, Sm} where S denotes staff i.e. S = {S1, S2, S3, …} where Si is the i^{th} staff member having access to health data stored in cloud, Pt represents patients i.e. Pt = {Pt1, Pt2, Pt3, …} where P_{ti} is the i^{th} patient having access to only his or her record, D denotes data store and S_m security manager. The problem lies in how S and P_t interact with the entity D and how access to D is restricted by the component Sm.

B. Data Management Problem

Health data usually contains records spanning across hundreds of GB's of data. This data is usually difficult to manage using traditional tools and techniques available at disposal. Thus, we need a system that can handle such data characterized by large volume and variety. In order to meet this end the proposed technique uses health data management system which has been built over cloud database management system architecture.

C. Biometric Security management problem

The data stored at a third party location is prone to intrusive attacks, thus we need a management system to secure the system from such attacks. The two main objectives are to provide proper access to legitimate users and to authenticate the users (patients and staffs). The authentication is provided through the biometric authentication agent incorporated in the system. This agent also provides access control to users, so that no outsider or attacker is able to access the system with malicious intentions.

III. LITERATURE SURVEY

A. multimodal biometric system using fingerprint, face and speech

A biometric system which relies only on a single biometric identifier in making a personal identification is often not able to meet the desired performance requirements. Identification based on multiple biometrics represents an emerging trend. We introduce a multimodal biometric system, which integrates face recognition, fingerprint verification, and speaker verification in making a personal identification. This system takes advantage of the capabilities of each individual biometrics. It can be used to overcome some of the limitations of a single biometrics. Preliminary experimental results demonstrate that the identity established by such an integrated system is more reliable than the identity established by a face recognition system, a fingerprint verification system, and a fingerprint verification system.

B. Evaluation of Automated biometric based identification and verification system

Recent advancements in computer technology have increased the use of automated biometric-based identification and verification systems. These systems are designed to detect the identity of an individual when it is unknown or to verify the individual's identity when it is provided. These systems typically contain a series of complex technologies that work together to provide the desired results in turn, evaluating these systems is also a complex process. The authors provide a method that may be used to evaluate the performance of automated biometric-based systems. The method is derived from fundamental statistics and is applicable to a variety of systems. Examples are provided to demonstrate(clr) the practicality of the method.

C. Biometric identification system based in keyboard filtering

We have revised several authentication systems based on biometric technology to resume advantages and disadvantages. Because pure hardware biometric systems of user authentication have low rate on results over computational and economic cost, alternate biometric methods of low Computational cost based on software development, are also being evaluated. We have developed a first prototype of a software system to elicitate (to call forth or draw out (something, such as information or a response) — elicit in a sentence.) sets of 20 password stroke samples, named attacks, with a population of 10 different users totaling 200 attacks. The results obtained demonstrate that users follow generally certain patterns when they are writing their password, and is possible to reinforce the user's password authentication method by means of the analysis of user stroking patterns. In addition it is necessary to increase the population size and number of samples to establish standard and reliable rules. Finally, it is very difficult to find a general user pattern applied to every password.

D. Biometric identification system based on Eigenpalm and Eigenfinger features

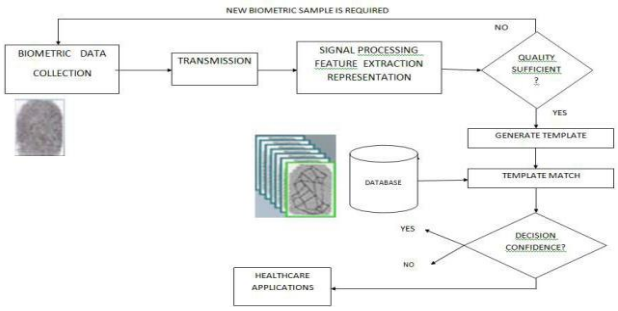
This paper presents a multimodal biometric identification system based on the features of the human hand. We describe

a new biometric approach to personal identification using eigenfinger and eigenpalm features, with fusion applied at the matching-score level. The identification process can be divided into the following phases: capturing the image; preprocessing; extracting and normalizing the palm and strip-like finger subimages; extracting the eigenpalm and eigenfinger features based on the K-L transform; matching and fusion; and, finally, a decision based on the (k, l)-NN classifier and thresholding. The system was tested on a database of 237 people (1,820 hand images). The experimental results showed the effectiveness of the system in terms of the recognition rate (100 percent), the equal error rate (EER = 0.58 percent), and the total error rate (TER = 0.72 percent).

E. A hybrid fusion method of fingerprint and identity for higher security application

Though fingerprint identification is widely used now, its imperfect performance for some high security applications, such as ATM, the access control of nuclear power stations and exchequers, etc, is still a challenge. In high security applications, an extremely low false accept rate and as low as possible false reject rate are desired at the same time, which is called Double Low problem in this paper. It is to be noted that even a fingerprint system with very low equal error rate cann ot achieve such a Double Low goal. It is difficult to solve Double Low problem only by improving the performance of a certain individual fingerprint identification algorithm, and the fusion of various fingerprint identification algorithms becomes a promising way. In this paper, a hybrid fusion method of fingerprint identification is proposed to solve Double Low problem. Firstly, minutiae-based and ridge-based matching algorithms are used orderly, which is a kind of serial fusion strategy. Secondly, a rank-level fusion is used, which is a kind of parallel fusionstrategy. Experiment results on FVC2002DB1 and FVC2002DB2 indicate that only 6.6% fingerprints are falsely rejected on the average under zero false accept rate with our method, while 14.8%, 9.4% fingerprints are falsely rejected under zero false accept rate with the serial fusion strategy and the parallel fusion strategy, respectively.

IV. ARCHITECTURE DIAGRAM



CASE STUDY: HEALTHCARE CENTER AT CAPITAL CITY OF A DEVELOPING COUNTRY

In a developing country like India with the population mark reaching second highest in the world. Health is an issue of prime concern as the individuals are the nations building forces. The capital city itself has a population of approximately 1780 lakh. Lakhs of patients visit healthcare centers and corresponding to each patient a record is maintained. According to department of health and family welfare, the department has to cater to the needs of approximately 160 lakh . people plus migratory and floating population from neighboring states. With the evolution of digital era a digital copy is kept and since the numbers of patients escalate on a daily basis therefore this has lead to huge volumes of healthcare records. Therefore, it's the need of the hour to handle such voluminous records.

A. Health Data Management System

This component of the healthcare cloud is responsible for management of patients report and other information. It is composed of three layers namely client level, health service provider level and data center level. The health service provider level is further divided into administrative and security level. Biometric authentication agent acts at the security level. Client level provides an interaction interface between the cloud data and its users. The security and resource provisioning is in turn handled by the two components of health service provider level respectively. The data storage and its management is the responsibility of the data center level. Thus, the Health Data Management System is responsible for overall management, storage and retrieval of the healthcare data.

B. Biometric authentication agent

This module uses biometric signatures for the purpose of authentication. The dynamic features of a signature is captured using a digitizing tablet which records features like x, y coordinates, velocity of the pen, total time taken to sign, angles of pen while signing, number of pen ups and pen-downs, acceleration etc. After the signature is captured its important features are extracted and then it is preprocessed and stored as a template. After this phase, this template is used for training the data and then these trained networks are stored in cloud. During verification phase, the user's signature is checked against the stored database and it is found out whether the user is genuine or forged. Moreover, another added advantage of this approach is that the processing is also done on cloud. This saves on the storage and cost along with providing lesser carbon footprints i.e. it's an energy efficient approach as it makes use of mobile and handheld devices like tablets and phones for access purpose.

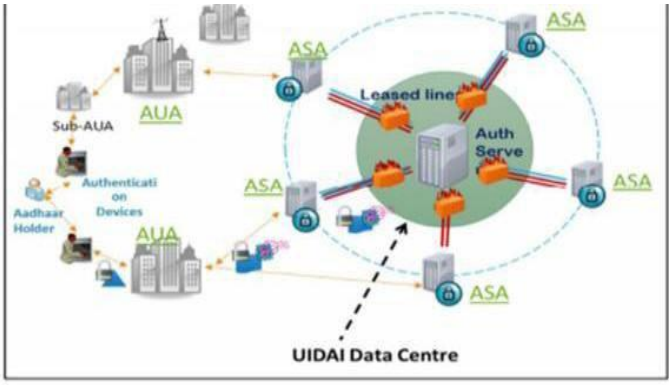


Figure.3.UDAI architecture framework

V. METHODS & MATERIALS

Biometrics and Aadhaar card can be characterized as a quantifiable physiological and behavioral characteristic that can be thusly compared & captured with another case at the time of individual confirmation. These innovations are a protected method for authentication since information of both advances are one of a kind, can't be shared, can't be replicated and can't be disregarded. GSM is utilized for making an impression on higher powers when unique mark and Aadhaar card acknowledgment false likewise sort wrong secret key. Our project idea secures the individual data with least hazard factor. Proceed with it, it gives a solid secret pass word to the

usage of it by the system administrator. We can utilize one this system framework in large scale in all medical and health care institutes with more security.

Proposed System: The Biometric characteristics of each and every individuals dwelling in the globe along with their personal details like name, address, contact number and parents details would be feed into centralized database server. In case of any accidents the health care centres make use of BMAD, obtains the biometric patterns and feed the obtained patterns into common proposed Website, which in turn connected with centralized Aadhar database server.The obtained biometric pattern would be matched with the existing biometric pattern of Aadhar database, If the Biometric patterns matches ,the centralized server displays the details about the individual (with his/her family members contact numbers) to the health care centres through which the request for individual identity were been made. The Health care centres as to take of the responsibility for alerting the family members of the individual, whom had met with an accident through SMS services or through a phone call.

Figure.4. functioning of proposed system

VI. MODULE AND DESCRIPTION

A.PATIENT MANAGEMENT SYSTEM: In the module of the patient management system, there is a facility to register patients and view their reports and history. Patient management system allows getting detail information of patient's health condition.

B.DOCTOR SERVICE REPORT SYSTEM: Doctor Services Report System allows getting complete information and management about the services of doctors. In these report details of doctors such as their specialization field, their work efficiency, and their duty hours and many other details and information could be managed by the management.

C.MEDICAL SERVICE MODULE: Medical Services System allows adding a list of services that are provided by the hospital such as dental treatment service, cardiac services, mental treatment services, bones treatment services and much more. The patient is able to view the list of services and departments offered by the hospital along with all other details of treatment. It also manages the service timing, emergency services according to the condition of the patient.

D.BMAD MODULE: Biometric Authentication device (BMAD) captures biometric characteristics of an individual and the obtained data's were passed to the AADHAR database.

E.DATABASE MODULE: Database has various demographic (like Name, Address, DOB, Gender, mobile number, email) and biometric information (fingerprint scan, facial scan, retinal scan, iris Scan) of all citizens resides in the nation.

VII. AUTHENTICATING USER ACCESS

In order to ensure that regular users have to access the data stored on healthcare cloud we use the proposed biometric authentication technique only. In order to speed up the processing use parallelized technique though Map Reduce which is based on hadoop framework? Popular technique is called hadoop for parallel processing of large date on cloud. Authenticating the access to healthcare data use mobile phones to ensure that the all process is energy and cost efficient.

TABLE.1. HEALTH DATA USERS AND THEIR PROPERTIES

USER TYPES	PRIORITY
VIP Patients	3
Privileged Patients	2
Privileged Staff	4
Regular Staff	1

The proposed approach is divided into two phases: Environment and Authentication phase

ALGORITHM 1
ALGO Health Security Check
Input: P: user priority which can be either 1, 2, 3 or 4

1. Begin:
2. **If P equals 1** */* If a user is a regular staff then authentication is performed with low priority*/*
3. Then
4. **ALGO Health Authentication**(Priority_Low)
5. End If
6. **If P equals 2** */* If a user is a privileged staff then authentication is performed with average priority*/*
7. Then
8. **ALGOHealthAuthentication**(Priority_Avg)
9. End If
10. **If P equals 3** */* If a user is a privileged*
11. *patient then authentication is performed with high priority*/*
12. Then
13. **ALGOHealthAuthentication**(Priority_High)
14. End If
15. **If P equals 4** */* If a user is a VIP patient then authentication is performed with very high priority*/*
16. Then 16.

ALGOHealthAuthentication(Priority_VHigh)

17. End If
18. End

Phase 1- Environment phase
In this phase, the staff and the patients together in the healthcare centre are enroll themselves by signature samples using either the capturing signature device or their smart phones that are installed with the capturing software. Once captured the user's signature, the quality of the given

signature is checked using SigQuality software. The function of this software is the samples signature match up to quality required for authentication. Once this is matched, samples are extracted and are stored in the healthcare cloud.

Phase 2-Authentication phase

The user has signature, which is sent to quality check and features are extracted. Then sample signature is checked against the stored user template in the healthcare cloud. This is performed using resilient back propagation algorithm in feed forward neural network. To find out whether the user is genuine one or not then matching process is done. ALGO Health Security Check describes performing security check on health data lying in the healthcare cloud. This hierarchy is based on priority of users. Priority value is assigned at the time of enrollment on a scale of 1-4, lowest priority value is 1 and highest value is 4. The different types of users and their priority values are shown in Table.

ALGORITHM 2

ALGO Health Authentication

Input: L: number of users, M: number of signature samples of each user, P: Threshold value taken as input from ALGO Health Security Check **Target**: target matrix **Output:** TNet : trained network

1. Begin:
2. **ParFor** j = 1 to L
3. **ParFor** k = 1 to M
4. **ReadSamples**( ) */*Input signature samples from individuals for authentication purpose*/*
5. End ParFor
6. **End ParFor**
7. Od=**Sigmapreduce** (Id, Sigcovariancemapper, Sigcovariancereducer) */* Running Sigmapreduce on input data samples */*
8. Cov = **Sigcovariance**(Od) */*covariance is calculated on the data output from Sigmapreduce */*
9. S = sqrt(**diagonal**(Cov)) */*square root of the diagonal elements of the covariance matrix obtained from previous step is calculated */*
10. Cor = Cov/s*s' */* correlation from covariance matrix and product of square root matrix obtained from step 10 and its transpose is calculated */*
11. Pcacoef ← svd(Cor) */* PCA is performed using singular value decomposition on the correlation matrix obtained from step 10*/*
12. Parallelized training:
13. **For** j = 1 to L
14. For k = 1 to M
15. Input1ij ← Pcacoefij */* inputting preprocessed signature samples obtained from step 11*/*
16. End For
17. **End** For
18. TNet = Φ */*Empty trained network in the beginning*/*
19. For l ϵ Loc **do** */* repeating steps 20-22 for all the local networks*/*
20. Tloc= **netcreate**() */*Creating local networks using Resilient backpropagation algorithm on a feedforward neural network in a distributed manner */*
21. (Tloc, Err) = **Sigtrain**(Tloc ,input, target, P) */* Performing training on local networks created in step 20*/*
22. TNet ← Tloc ∪ TNet */* Combining all the local networks to form a combined network TNet */*
23. End For
24. End of parallelized training
25. **Return** TNet */* a combined network TNet is returned at the end of parallelized training*/*
26. **End**

Level of security quaranteed by priority value associated with the user. This is taken care of by associating a threshold value in the training algorithm depends on priority P. This algorithm authentication is performed based on the associated priority value. If staff member accesses the data by user with low priority then its authentication performed with its threshold value set to Priority_Low. Similarly values are set as Priority_Avg, Priority_High and Priority_VHigh for privileged staff, privileged patients and VIP patients respectively. Authentication of the health data based on the threshold value jk feature extraction. Back propagation training of multilayer feed-forward neural networks using resilient backpropagation. It involves chain rule to findout the impact of each weight in according to error function. "Vanishing gradients" problem solved by RPROP which with complexity of an artificial neural network and increase in depth, stochastic gradient descent propagates gradient Algorithm becomes increasingly smaller which leads to negligible updates in weight. Fixed update value δ_{ij} is achieved. η is an asymmetric factor. The decrease or increase in values depends on the gradient sign change with respect to weight ω_{ij} converges to a local minima. Psuedocode of resilient back propagation algorithm Δ_{ij} is the update value for each weight i.e. Δw_{ij} is the change in weights. Δ_{min} and Δ_{max} are the minimum and maximum change.

Definition 1: Resilient propagation algorithm implemented by net create function on a feed forward network in a distributed manner and uses size of the dataset done by this distribution.

Definition 2: Resilient propagation algorithm uses sigtrain function which back propagation algorithm using sigtrain function which takes target matrices and input and network based on the architecture of a local network created.

Theorem 1: *The time complexity of ALGOm Health Security Check is O(L xM).*

Proof: The time complexity for performing security check on health data stored on cloud is O (L x M). It takes O (L x M) for performing security check on low priority users (line 4, ALGORITHM 1) as given in theorem 2. It takes O (L x M) for performing security check on average priority users (line 8, ALGORITHM 1). It takes O (L x M) for performing security check on high priority users (line 12, ALGORITHM 1) and takes O (L x M) for performing security check on very high priority users (line 16, ALGORITHM 1).Thus, the complexity of ALGOHealthSecurityCheck is maximum (O (L x M), O (L x M), O (L x M), O (L x M)) i.e. O (L x M)

Theorem 2: *The time complexity of ALGO Health Authentication is* O (L x M) *where L is the number of users and Mis the number of signature samples* **Proof:** For performing authentication of health data the complexity is *O (L x M).* It takes *O (L x M)* for performing read on sample data *(line 4,* ALGORITHM 2), It takes O (L *x M)* for performing mapreduce function on data samples *(line 7,* ALGORITHM 2*).* Sigcovariance finds the covariance in O(L2) time and steps 13-17 take O (LxM) time and steps 20-21 takes O(LxM) time. Thus, the complexity of is done by ALGO Health Authentication algorithm. I_d is the input sample signature matrix which represents k^{th} samples of j^{th} user. Parallelized approach ensures that all the processing of data is done across distributed cluster by usage of mapreduce

framework. This processing speed is high effective cost along with fault tolerant. Input data is performed PCA ALGO Health Authentication is maximum (O (L x M), O (L xM), O (L2), O (L x M), O (L x M)).

VIII. RESULTS

From review of previous research studies, we may come to a conclusion that the growth in the electronic transaction scheme has resulted in a greater demand for accurate & fast user identification and authentication. An embedded fingerprint biometric authentication scheme for individual identity in health care systems is proposed in this paper. Along with AADHAAR CARD authentication for more security; also included in this paper. Finally, positive and accurate results can be drawn out after observing the AADHAR CARD & Fingerprint Biometric Authentication scheme results

IX. CONCLUSION

In upcoming future, if the system proposed comes to real time existence, it saves time in medicinal centre and it highly reduces complexity of identifying individuals during critical emergencies like accidents, death and so on. This system provides accurate information about an individual, whenever in need and it is universally accepted.

X. REFERENCES

[1]. D. Munro, "New Study Says Over 2 Million Americans Are Victims Of Medical Identity Theft - Forbes." [Online]. Available: http://www.forbes. com/sites/danmunro /2015/02/23/new- study-says-over-2-million-americans-are-victims-of-medical- identity-theft/#640dcc93702d. [Accessed: 18-Aug-2016].

[2]. L. Shin, "How biometrics could improve health security," *Fortune*, Feb-2015.

[3]. D. Borthakur, "HDFS architecture guide," *Hadoop Apache Proj. http//hadoop apache …*, pp. 1–13, 2008.

[4]. A. Jayanthi, "7 celebrity data breaches: When employees snoop on high-profile patients," *Beckers Health IT and CIO Review*, 2015.[Online].Available: http://www. Becker shosp it alreview. com/ healthcare- information-technology/7-celebrity-data-breaches-when-employees-snoop-on-high-profile-atient s.html.[Accessed: 19-Aug-2016].

[5]. M. Alam and K. A. Shakil, "Cloud Database Management System Architecture," *UACEE Int. J. Comput. Sci. its Appl.*, vol. 3, no. 1, pp. 27–31, 2013.

[6]. B. Feldman, E. M. Martin, and T. Skotnes, "Big Data in Healthcare Hype and Hope," 2012.

[7]. P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology."

[8]. A. O"Driscoll, J. Daugelaite, and R. Sleator, "„Big data", Hadoop and cloud computing in genomics," *J. Biomed. Inform.*, 2013.

[9]. A. Rosenthal, P. Mork, M. H. Li, J. Stanford, D. Koester, and P. Reynolds, "Cloud computing: A new business paradigm for biomedical information sharing," *J. Biomed. Inform.*, vol. 43, no. 2, pp. 342–353, 2010.