International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

A Secured Data Retrieval Architecture for WBAN using Elliptic Curve Digital Signature

M.J. Bharathi, V.N. Rajavarman, R. Shobarani

Abstract:*The big data is proposed a secure scheme of data collection that to deal the problems in WBAN (Wireless Body Area Network). To start with to register the sensor nodes using CA (Certification Authority) connect the Network of Big data center. After the preprocessing stage, the sensors are correlated with big data center through authentication on both sides by ECDSA (Elliptic Curve Digital Signature Algorithm). The sensor node designed using distributed storage and the collected data transfer with improved security protection.*

Keywords: Wireless body area network, Elliptic curve digital signature algorithm, Certificate Authority, Sensors, Hadoop

I.INTRODUCTION

Many modern industries developed by using new innovative networking and wireless technologies to secure the data efficiently. Wireless Body Area Networks act as a wireless network, its purpose to communicate between different sensor nodes around the human body to monitor the body parameters and movements. Transmission of data in wireless networks is critical. To assure the security future in WBAN we proposed ECDSA based authentication scheme that provide secure and authentication protection in big data distributed storage.

[1]Chunqiang Hu, et.al designed a secured data communications between the wearable sensors by using Ciphertext-Policy Attribute Based Encryption and also design to retrieve the sensitive data by provides message authenticity and collusion resistance. TinyZKP[2] proposed on TinyOS-based sensor nodes, also measured authentication schemes to run faster and reduced the energy cost. [3]Amrita Roy, et.al focused on light weight applications Between the nodes in network and produced the properties of preimage resistance and collision resistance. [4]Amrita Roy, et.al defined the Wireless sensor networks, reduce the communication and computational costs based on signature scheme with message recovery/verification process securely.

[5]Sanskruti Patel, et.al discussed the performance of tools used in health care in Big data analytics. [6] Isabel de la Torre, et.al deals with different techniques helps to carry out the cryptography methods and protocols for analyzing the data sharing. [7]Muhammad Sheraz Arshad Malik, et. al produced the utilization of different security and privacy requirements in cryptographic algorithm in WBAN .

II.SYSTEM ARCHITECTURE

The word Big Data wrappers distinct technologies similar as cloud computing. The input of huge data getting from Social Networks like Facebook, Twitter, LinkedIn, etc., Among frequent others, to analyze the Big Data in an efficient manner using Architecture as shown in Fig.2.1 describe n number of satellites that acquire the earth perspective big data envisions with sensor nodes or perspective cameras through which properties are traced by emission. Unique approach are adapted to process and transliterate remote sensors nodes for the purpose of generating resource surveys, etc. There are remote sensing Big Data architecture split into three parts, i.e., 1) Cloud Data Processing (CDP) 2)Big-data Storage Unit(BSU) and 3) Health Care Big data Retrieval Unit(HCBRU).

Manuscript published on 30 August 2019.
***Correspondence Author(s)**
M.J. Bharathi, Research Scholar, Dr. M.G.R. Educational and Research Institute
V.N. Rajavarman, Professor & Deputy Dean , Dr. M.G.R. Educational and Research Institute
R. Shobarani, Professor, Dr. M.G.R. Educational and Research Institute

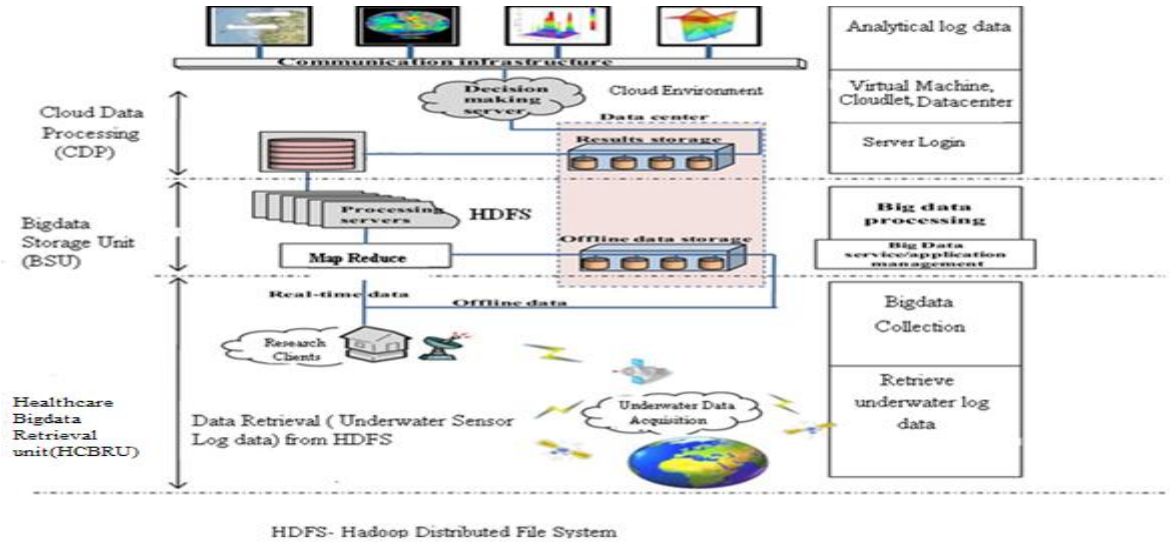

Fig. 1 HDFS- Hadoop Distributed File system

Cloud Big-data Processing (CDP)

Irrelevant sensing elevates the evolution of earth observatory system as cost effect and parallel data achieve system to satisfy the compensative needs. The earth and space science society primarily approved the results as conventional for parallel processing in the precise circumstance. As satellite tools for earth observation incorporated more enlightened qualifications to accumulated big data acquisition. Hence the need for parallel processing, the required of huge data which could effectively analyze the big data, for that, the Secured architecture is introduced in the remote sensing that gathers the data from various satellites around the globe as shown in Fig. 2.1. Various atmospheric gases and dust particles observed the raw data and suspect that the satellite can conclusive the defective data. To execute efficient data analyzes remote sensing satellite preprocessing data governed by many situations to include the data from various sources, which not only reduces the storage unit, but also enhances analyses in accuracy and then the accumulated information are directed into a ground station using downlink channel with an appropriate tracking antenna and communication link in a wireless atmosphere. The data must be improved in dissimilar methods to remote deformations caused due to the progress of the platform attitude, earth curvature, incomparability of irradiation, variations in sensors distinctive, etc. The data is then communicated to earth base station additional preprocessing using direct exchanging information link. The determined data, converting measure into two steps are processing the big data in real time and offline. In the process of offline, data center received the data from earth base station for depository used for future estimate. In spite of that the real time data processing, it reduce the processing time and directly communicated to the filtration and load balancer server.

Big-data Storage Unit(BSU)

In Big-data Storage Unit (BSU), For data analysis, the useful information is identified by filtration and rests of them are discarded. Filtered data assign them into various processing servers allocated by load balancing server. The Filtration and load balancing algorithm implemented to segment the data that makes the performance of proposed system and generated the real time results in each segments for compilation, organization, and storing for further processing.

Health Care Big data Retrieval Unit (HCBRU)

HCBRU contains aggregation and compilation server, results storage server(s), and decision-making server. During the compilation, the partial results send by the processing servers in DPU for further processing and to store them. Our Proposed system used to compile, organize, store and transmit the results by supporting various algorithms during compilation. The compiled results used in any server to process at any time also send the copy of the result to the decision making server for taking the decision. The decision algorithm made by decision-making server, make the decisions on any disaster occurred so that it utilized by application to make their development.

Retrieval Number: J10600881019/19©BEIESP
DOI: 10.35940/ijitee.J1060.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

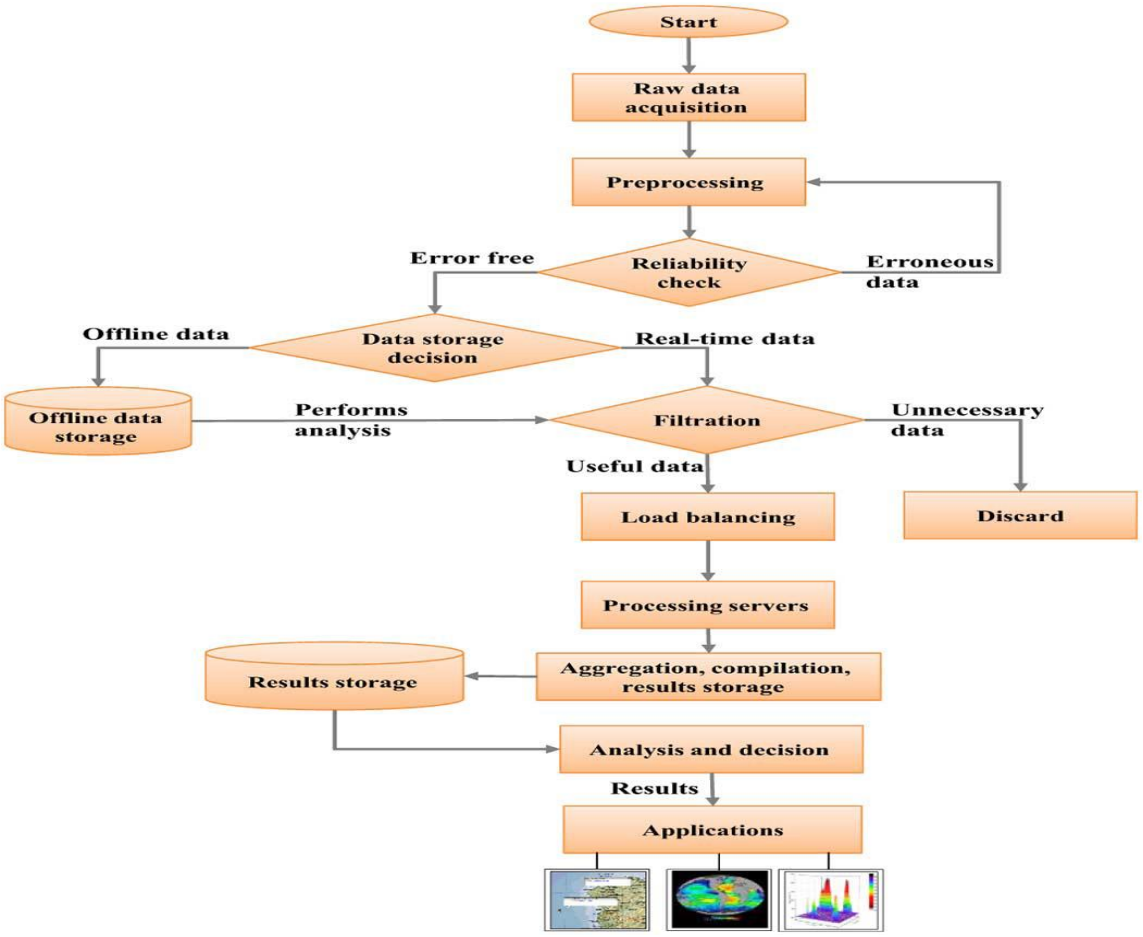

Fig. 2 Flowchart of the Big Data architecture

III.HADOOP ENVIRONMENT

The HADOOP platform was designed to solve problems where it has a mixture of complex data are not well arranged into tables. HADOOP is developed to perform huge machine but not to share in memory. while loading huge data into HADOOP the software partition the data into pieces then it spreads across different servers. HADOOP keep track of where the data exists. The server keeps multiple copies, the original remains in same, the duplicates goes offline Main nodes run Task-Tracker to accept and reply to Map-Reduce tasks, and also to store required blocks of .Data-Node as possible. Central control node runs Name-Node to keep track of HDFS directories & files, and Job-Tracker to dispatch compute tasks to Task-Tracker .

HADOOP Clustering

A hadoop cluster consists of main components as below, all of which are implemented as Java virtual machine daemons.

Job Tracker-Master node controlling the distribution of a Hadoop(Mapreduce) is responsible for scheduling the jobs on the various TaskTrackernodes. In case of node –failure, it scheduled on another node become free. The simplicity of Mapreduce tasks agreed that such restarts can be achieved easily.

Name Node- Node controlling the HDFS. HDFS responsible for fault-tolerance and allocating any component that needs access to files. Usually, fault-tolerance is achieved by replicating the files with one of the node being an off-track node over three different nodes.

TaskTracker- It requests and updates reports of allocated work until user code is malicious. The job is not run by its TaskTracker daemon but forks a separate daemon for each task instance.

Data Node- The node and files keep on the HDFS and these node also work as TaskTrackers. The Job Tracker strive to allocate work to nodes such files accesses are local as possible.

HDFS (HADOOP Distributed File System)

The Files are split into blocks and each Block divide across many machines at load time (Different machines have different blocks of keeping same file). Blocks are repeated across different machines and to track the file stored in NameNode.

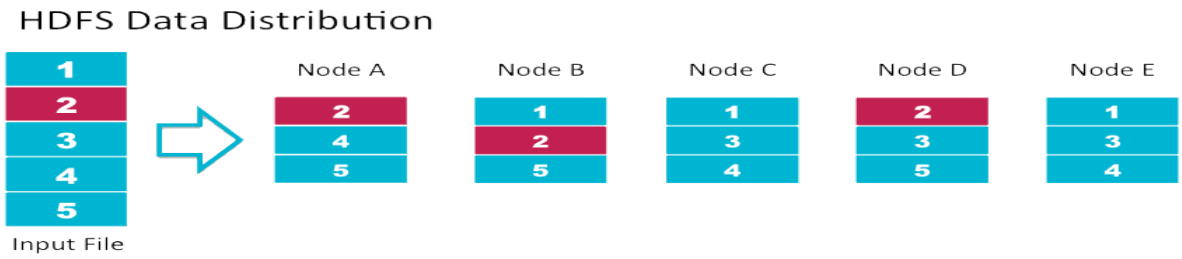

Fig. 3 Files are stored in HDFS

Proposed ECC Protocol

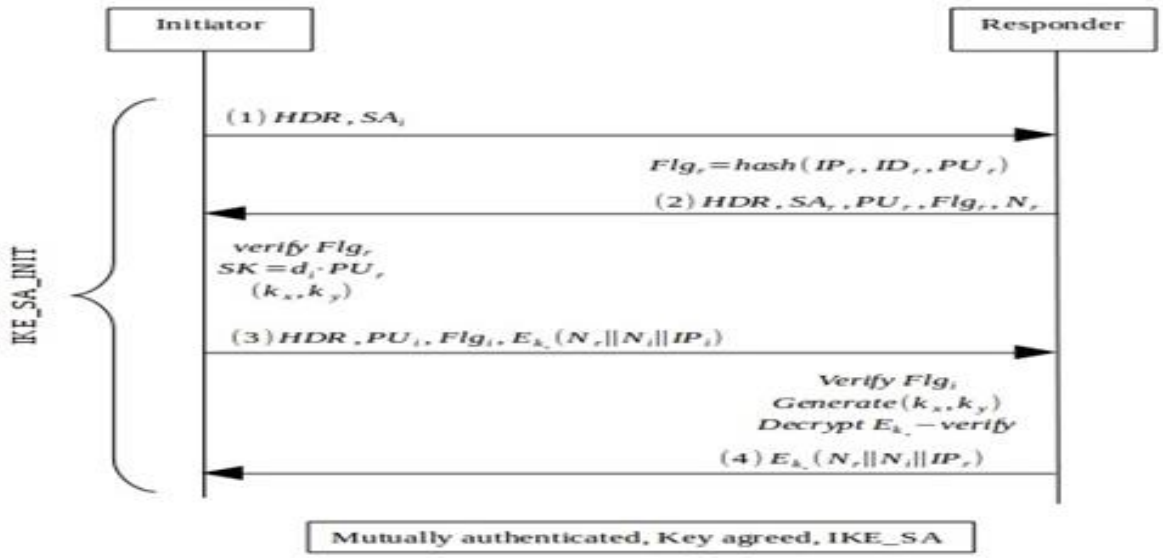

Fig. 4 Elliptic Curve Cryptography Certified protocol

IV.PROPOSED ALGORITHM

Proposed Elliptic Curve Cryptography Certified Protocol

Session key Generation in Encryption

Algorithm send_msg (ZP, ID, PU)
{
Initialize flg for receiver;
Hash(IP,ID_r,PU);
Responder send HDR,SA,PU_r,Flg,N_r;
return flg $_r$;
}
Algorithm Verify(Flg r, PU r)
{
Initialize flg r from responder to Instructor;
Verify Flg r using Key Generation;
Generate Key pairs for Verification;
}
Algorithm Encryption(flg r,key x,key y)
{
Mutually authenticates key agreement verify Flg i Generate (Kx, Ky);
$E_k(N_n,||N_j||P_r)$;
return Flg i
}
HDR-Header
SA-Security Association
Flg_r – flag for receiver
IP—Address
PU-public key
ID—Device ID

V.CONCLUSION AND FUTURE WORK

In this paper, we propose a protocol based on elliptic curve cryptography certified algorithm to secure the efficient data communication with one time token to assure the encryption algorithm efficiently and also to reduce the cost. In future work to enhance the new approaches to analysis the performance of secured data.

REFERENCES

1. Chunqiang Hu, Hongjuan Li, Xiuzhen Cheng and Xiaofeng Liao, "Secure and Efficient data communication protocol for Wireless Body Area Networks", IEEE Transactions On Multi-Scale Computing Systems, Vol. , No. , 11. 2015
2. Limin Ma · Yu Ge · Yuesheng Zhu, " TinyZKP: A Lightweight Authentication Scheme Based on Zero-Knowledge Proof for Wireless Body Area Networks", Wireless Pers Commun (2014) 77:1077–1090
3. Amrita Roy Chowdhurya , Tanusree Chatterjeeb , Sipra DasBita," LOCHA: A Light-Weight One-way Cryptographic Hash Algorithm for Wireless Sensor Network". The 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014).

4. Kyung-Ah Shim, Young-Ran Lee ⇑ , Cheol-Min Park," EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks", SciVerse ScienceDirect, Ad Hoc Networks 11 (2013) 182–189
5. Sanskruti Patel and Atul Patel," A Big Data Revolution In Health Care Sector: Opportunities, Challenges And Technological Advancements", International Journal of Information Sciences and Techniques (IJIST) Vol.6, No.1/2, March 2016
6. Isabel de la Torre, Begoña García-Zapirain, Miguel López-Coronado," Analysis of Security in Big Data Related to Healthcare," Journal of Digital Forensics, Security and Law Volume 12 | Number 3 Article 5
7. Muhammad Sheraz Arshad Malik, Muhammad Ahmed, Tahir Abdullah, Naila Kousar, Mehak Nigar Shumaila" Wireless Body Area Network Security and Privacy Issue in E-Healthcare", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 4, 2018
8. Manikanthan, S.V., Padmapriya, T, A secured multi-level key management technique for intensified wireless sensor network. International Journal of Recent Technology and Engineering, V.7, No.6S2, 2019