International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Implementation of Digital Signature Algorithm using Big Data Sensing Environment

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

Abstract: ***WBAN is a self-governing and perceptive used to informant the activities of a person and to improve the individuality of people, which satisfies the requirements of the user's needs. In this paper, we propose a Big data retrieval unit in WBAN using Elliptical Curve Cryptography. Big data transmit the data through Map reduce and retrieve the data safely using ECCDS algorithm. Map-reduce is a programming method for accessing multiple data sets on multi-node hardware efficiently using a distributed storage process and it incorporate the entire in-between requirements connected via the identical in-among key in . Cloud Sim extensible toolkit is used to enable the modeling and to enhance the application provision***.

Keywords: Map reduce algorithm, Hadoop, Cloudsim Architecture, WBAN Architecture

I. INTRODUCTION

[1]Mapreduce be an "encoding portrayal just as an associated achievement expected for regulation with produce gigantic datasets". Map reduce was intended to deal with entanglements of a conveyed framework like obligation acknowledgment, transfer adjusting, information allotment, and task parallelization. And an undemanding as of recently controlling structure with the aim of lets the software engineer composes inconvenience free units of exertion as a map and reduces capacities. The commitment esteems are mapped into set of transitional worth pair. Maps are a different errand that reforms the heap hubs into transitional hubs. Every transitional hub corresponds with the yield key that is therefore masterminded by the development and transport to the reducer to modify the end generation. The reducer partitioned the output once it sorted. [2]The task of Map-Reduce is achieved by storing more files and working with a read-write operation that is accomplished by these activities. [2]Proposed a Word Count application of Map reduces divides input file into tokens in the form of key value. [4]ECC provide smaller key sizes with less complexity but same level of security comparative with other public key cryptosystem concern uses of larger key sizes in greater complexity. [5,8]Secure cloud storage system using ECC for encryption is better than AES with many security and privacy attributes like integrity, Storage, confidentiality, privacy-preservability, availability, accountability and vulnerability.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
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

[6]ECC demonstrate as the finest cryptographic technique for securing unauthorized medical technique and data transmission in a restrict environment. [3]CloudSim is a superior model pack for vitality inclining server farm appraisal in dynamic circumstance.[7] Various innovations have demonstrated their proficiency in continuing WBANs applications, for example, blocked off observing, biofeedback and help wellspring of income by reacting to their exact quality of service (QoS) necessities.

II. WBAN ARCHITECTURE

For productive method for information transmission, the remote innovations and sensors are imparted by means of base station. The varying restorative and non-medicinal applications can be positive by the IEEE 802.156 utilizing the moderate qualities. The examination such as data rate, intrusion created by the coincidence of different technology in the same position and needs of WBAN applications are resolved by acceptable radio technology**.**

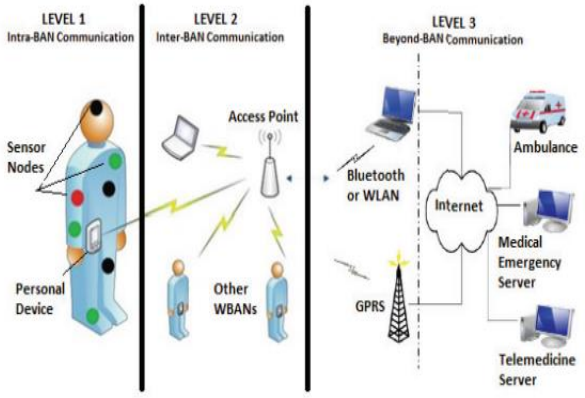

Fig. 1 WBAN Architecture

III. CLOUD ARCHITECTURE

The CloudSim simulation layer is used for modeling and simulation of virtual cloud based data center environment counterfeit including dedicated management interface for memory,VMs, band width and storage. Fig 2 delineate like a Cloud registering structure that made out of administration shoppers (SaaS suppliers), expediting and suppliers, organizer benefits that assurance the utility-driven between systems administration of mists application provisioning and remaining task at hand entry.

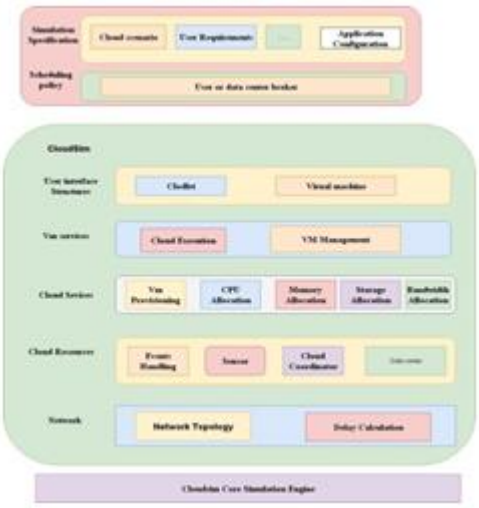

Fig.2 Architecture of Cloud Environment

The arrangement of VMs is allotted by a cloud have in incidental and its applications are sent on SaaS suppliers at the QoS level. The functionalities of this layer additionally disclosure by permit a Cloud application layer to achieve multifaceted outstanding burden profiling and application execution study.

The User code is the essential layer in Cloud Sim assault that shows the fundamental substances for has (with details, number of machines, etc.,), applications(necessities and measure of tasks), numeral of clients, VMs and their sorts with counselor advancement strategy.

IV. MAP-REDUCE FRAMEWORK

Map-reduce is an encoding portrayal and an associated achievement for managing out and create enormous datasets. Fig. 3 gives the activity of a Map-reduce structure. Map-reduce was planned to hold confusions of a dispersed assortment like obligation resistance, load adjusting, information appropriation, and assignment parallelization. This is a simple framework enabling the programmers to present their work units in terms of map and reduce functions. The structure automatically takes worry of parcel and parallelizing duties on an immense measure of bunch modest help hardware. The Input value pairs mapped into a set of intermediate value pairs are known as mappers. These yield of mappers are organized and then divided by reducer.

Fig. 3 Map-reduce Framework

V. PROPOSED SYSTEM

The intensify in the information rates produce in the advanced universe is expanding exponentially. With a view in utilize existing contraption and innovation to inspect and collect, a tremendous amount of information isn't sufficient since they can't take out fundamental representation informational collections. In this manner we need to execute a structural proposition for dissecting both secluded path in disconnected and real occasion.

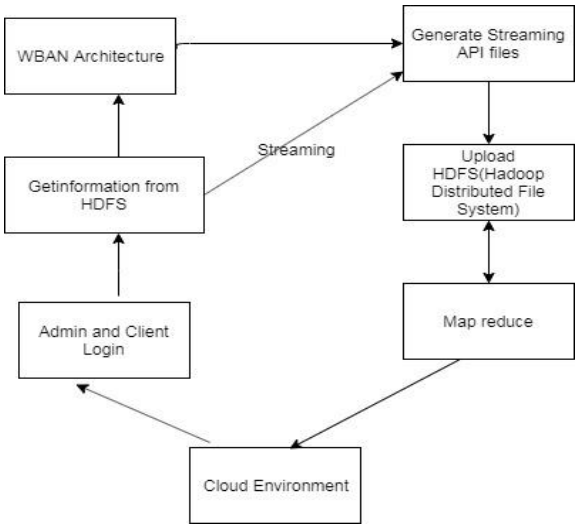

Fig. 4 Proposed Architecture

VI. REAL-TIME BIG DATA SENSING ARCHITECTURE

Real Bigdata Sensing Architecture contains three significant bits; collection, treasury server results away server(s) and regulatory server.The Hadoop processed the partial outputs produced by aggregation and compilation server and it indicates the outcomes are prepare to compile, although the aggregated outcomes may be not in structured and compiled form. Thus we need to composite the related results and arrange them into an actual form for future processing and to load them.

VII. PROPOSED ELLIPTICAL CURVE CRYPTOGRAPHY BASED BIG-DATA RETRIEVALUNIT

Key Generation Algorithm:

ECDSA Key Generation composed of two pairs(x,y), x is declared as private key , assume to be integer and the public key y, is an elliptic curve point, where as private key x compute the public key y.

Algorithm Key-Generation

{
//problem description: to calculate key pair
//Input: Domain Parameter x(q,FR,a,b,g,n,k)

E-Eliptic curve created over Fq
P-Point of Prime numberE(Fq)
Y-Eliptic curve point
//Output: To Generate Key pair(Public,Private Key)
Select a random number d in the interval {1, m-1}

- Calculate Y=xy

Y- Public key x- Private key
}

Signature Generation Algorithm:

The performance of the ECDSA produces the (r,s) pairs that perform a digital signature. The solution tests the capacity of an IUT to generate correct signatures. To test signature generation, the ECDSA supplies ten messages to the IUT and it creates the respective signatures and transmits to ECDSA. The ECDSA validation is done by using aggregated public key to substantiate the signature.

Algorithm Signature – Generation

{//Problem description: to generate signature pair(r,s)
//input: Input message-m, Domain arguments D=(z,FR,a,b,G,n,k)
//output :pair of integer (r,s)
Rand(1,m-1)
Kp=(c1,d1);// (integer between 0 and z-1)
r=x 1 mod m;
if(r=0)
rand(1,m-1)
$i=k^{-1}$ mod m
$s=k^{-1}$ {h(n)+dr)} mod m;//
h-secure hash algorithm
if (s=0)
rand(1,m-1)
return (r,s)
}
}

Algorithm Signature Verification

{
// Problem description: to verify the signature
// input :signature (r,s) on message ,authenticated
Domain parameters d=(z,FR,a,b,G,n,k)
Public key -Y
S=rand(1,m-1)
r = rand (1,m-1)
$w=s^{-1}$ mod m and h(n)
u1=(h(n)*w) mod m
u2=rw mod m
u1p+u2Q=(c0,d0) and v= c0 mod m
if (v==r)
print "verified the signature",
else
print "Not verified the signature"
}

Session Key Generation in Encryption

To verify correct and incorrect signature for each mod size selected, the ECDSA creates a key pair (p,q) of which the private key p is used to indication number of pseudorandom messages of 1024 bits. The ITU expressed the messages, signatures, domain parameters and public key q values using signature verification and then attempts to verify the signatures and returns the results to the ECDSA, which compares the received results with its stored results.

Algorithm Transmit (ZP, ID, PU)

{
Initialize Flag for destination;
Hash(IP,ID_r,PU);
Receiver send HDR,SA,PU_r,Flag,N_r;
return Flag $_r$;
}

Algorithm Certify (Flagr, PUr)

{
Initialize Flagrfrom receiver to Sender;
CertifyFlagr using Key Generation;
Generate Key pairs for authentication;
}

Algorithm Encryption(Flagr, key p, key q)

{
Mutually certify key agreement validate Flagi Generate (Qp, Qq);
$E_k(N_n,||N_j||P_r)$;
returnFlagi
}

VIII. RESULT

The exhibition of proposed ECC depends on the quantity of ascribes and time taken to scramble and unscramble the document. The execution time of Proposed ECC is less think about Novel ECC and key approach traits based encryption. Security of ECC is high contrast with and key approach traits based encryption since encryption depends on security characteristics. The information proprietor can make and characterize new access arrangement dependent on conduct of client and history of the client. Fine got entrance control is accomplished relying upon get to strategy. User gets to benefits and classification is accomplished by common confirmation. User mystery key accountably accomplished by ECC based encryption secure the key clients. Information unhesitatingly is accomplished through trust based property basedencryption. Fig 5.Shows the examination of Execution time in various record size. Utilizing Proposed ECC related credits like chronicled information to diminish the execution time dependent on confirmation component. We proposed a novel arrangement utilizing Encryption, session key age and confirmation and decoding for moderating security issues, with diminished execution time. Utilizing the novel arrangement we watched a 12% diminishing execution time. As a piece of our future undertaking, we mean to limit stockpiling overhead calculation.

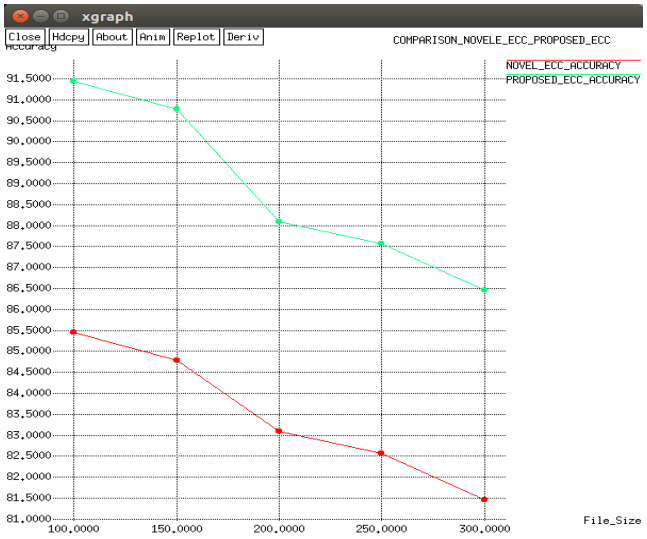

Fig. 5 Comparison graph

IX. CONCLUSION AND FUTURE WORK

Hadoop Map Reduce is a dispersed open-source programming structure to hold colossal datasets, the best approach to take care of the issue proficiently. The proposed method is used for generating a session key for acceptance and verification. During the execution, it generates the one time nonce without replication. Decryption algorithms to be defined in map-reduce function and the performance analysis is to be followed with a Novel ECC algorithm in the proposed ECC algorithm. User secret key accountably and data confidentiality is to be achieved by Nonce based encryption to protect the key users.

REFERENCES

1. VidyullathaPellakuri, Dr.D. RajeswaraRao,"Hadoop Mapreduce Framework in Big Data Analytics",International Journal of Computer Trends and Technology (IJCTT), volume 8 number 3– Feb 2014.
2. L. Greeshmaand G. Pradeepini,"Big Data Analytics with Apache Hadoop MapReduce Framework",Indian Journal of Science and Technology", Vol 9(26), DOI: 10.17485/ijst/2016/v9i26/93418, July 2016
3. Sajitha A V, Dr. A C Subhajini, "Analysis of Cloud Sim Toolkit for ImplementingEnergy Efficient Green Cloud Data Centers", International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 6 Issue IV, April 2018.
4. Weizhong Zhao, Huifang Ma and Qing He1, "Parallel *K*-Means Clustering Based on MapReduce", DOI: 10.1007/978-3-642-10665-1_71
5. JerrilMathson Mathew, Jyothis Joseph, "Parallel Implementation of K-Means Algorithm Using Hadoop", International Journal of Advances in Electronics and Computer Science, ISSN: 2393-2835, Volume-3, Issue-6, Jun.-2016
6. Shashi Kant Shankar, Anurag Singh Tomar, Gaurav Kumar Tak," Secure Medical Data Transmission by using ECC with MutualAuthentication in WSNs",4thInternational on Eco-friendly Computing and Communication Systems, Procedia Computer Science 70 (2015) 455 – 461
7. Rim Negra,,ImenJemili, AbdelfettahBelghith," Wireless Body Area Networks: Applications and technologies",ScienceDirectProcedia Computer Science 83 (2016) 1274 – 1281
8. S. Sridharan and A. Arokiasamy," Effective Secure Data Storage in Cloud by Using ECC Algorithm", Middle-East Journal of Scientific Research 25 (1): 117-127, 2017 ISSN 1990-9233© IDOSI Publications, 2017 DOI: 10.5829/idosi.mejsr.2017.117.127

AUTHORS PROFILE

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