iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XI **Month of publication:** November 2021

DOI: https://doi.org/10.22214/ijraset.2021.38995

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XI Nov 2021- Available at www.ijraset.com

Efficient Encryption Algorithm for Data Security in Big Data Cloud Environment

K. Praveen Kumar[1], T. N. S Padma[2], B. Ravi Raju[3], B. Pruthvi Raj Goud[4]
[1, 3, 4]*Assistant Professor, Dept. of Information Technology, Anurag University, Hyderabad, India*
[2]*Assistant Professor, Dept. of IT, Sreenidhi Institute of Science and Technology, Hyderabad, India*

Abstract: High speed Internet technology development and data technologies create a huge amount of information in day by day. Use of big data and cloud both are managing traditional data processing and storage issues. At the same time users can face many issues like data security and privacy manner. Here we proposed Blockchain based secure algorithm for to achieve Security and Privacy for big data.
Keywords: Security, Blockchain, Big data and Cloud environment.

I. INTRODUCTION

A. *Big Data*

Big data is a popular term that describes the growth and availability of data in both Structured and Unstructured data. That data is being generated from different data sources like digital systems, sensors & machine generated data, social media, online transaction processing systems and radio frequency data. This generated data need to processed and analyzed effectively with high rate.
By large or huge amount of data sets or big data, we means anything from a petabyte (1 PB=1000 TB) to an Exabyte (1EB=1000 PB) of data. Big data is classified in terms of 5Vs: Volume, Variety, Velocity, Veracity and Value.

Fig small data vs Big data

1) *Small Data:* Low volumes, batch velocities and structured varieties.
2) *Big Data:* Petabytes (PB) volumes, real time velocities and unstructured varieties. It is usually unstructured and qualitative nature.
a) Every second, there are around 9000 tweets on Twitter
b) Every minute nearly 600 comments are posted, 300,000 statuses are updated, and 140,000 photos are uploaded on face book.
c) Every 1 hour walmart, global discount department stores chain, handles more than 1 million customer transactions.
d) Every day consumers make around 12 million payments by using PayPal.

Here we observed us lives in digital world where data is increasing rapidly because of the user needs. Weather data is useful or not we produce huge amount of data at high rate. Big data is structured, semi structured or heterogeneous and unstructured in nature. It becomes difficult for computing systems to manage data because of high speed and volume at which it is generated.

Table 1: Security aspects in Big Data Life Cycle

Bid data 5V characteristics	Security Aspects				
	Confidentiality	Efficiency	Authenticity	Availability	Integrity
Volume		✓		✓	
Velocity		✓		✓	
Variety		✓		✓	
Value	✓		✓	✓	✓
Veracity	✓		✓		✓

B. Cloud Computing

Main issue that organizations face with the storage and management of big data is the huge amount of infra needed. To get the required Hardware setup and Software packages. These resources may be use maximum utilized or underutilized with the varying requirements. These challenges by providing a set of computing resources that can be shared through cloud computing.

1) These resources shared comprise apps, Storage solutions, networking solutions, development platforms and business processes.
2) The cloud computing environment saves costs related to infra in an organization by providing a framework.
3) In cloud platforms apps can be easily obtained the resources to perform computing tasks.
4) The cost of the acquiring these resources need to be paid as per the getting resources and their use of it.

Cloud computing is a transformative computing paradigm that involves delivering applications and services over the internet. Cloud computing involves provisioning of computing, networking and storages resources on demand and providing these resources as metered services to the users. Cloud computing resources can be provisioned on demand by the users, without requiring interactions with the cloud service provider. The process of provisioning resources is automated. Cloud computing resources can be accessed over the network using access mechanisms that provides platform independent access through the use of heterogeneous client platforms such as workstations, laptops, tabs and smart mobiles.

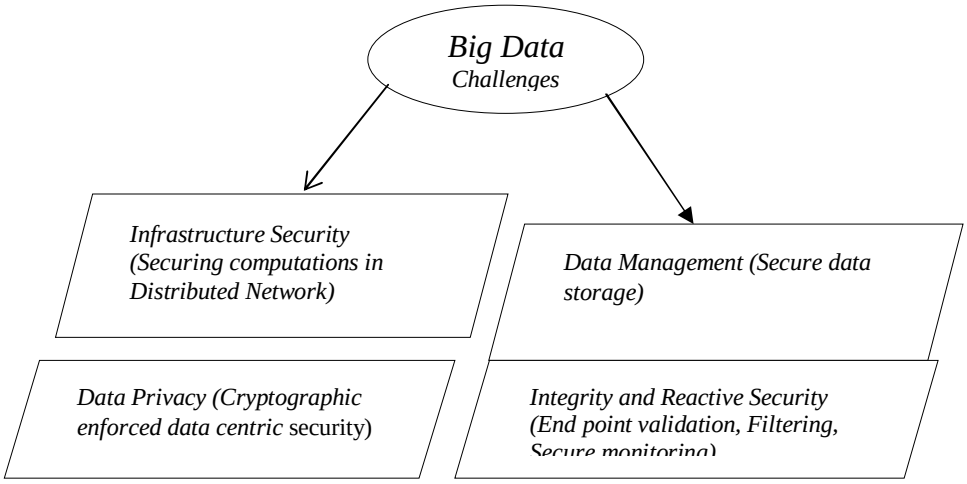
The Cloud Computing services are offered to users in different forms. Iaas (Infrastructure as a Service), Paas (Platform as a Service), Saas (Software as a Service).

C. Blockchain Technology

Consortiums are an association, of several participants such as banks, e-commerce, government agency, hospitals and so on. We can use blockchain technology to solve many problems and makes things faster and cheaper. Organizations like banks want to build a blockchain to make their needs easier, faster, and cheaper. In this situation, here are the things they need.

1) *Speed:* They need a blockchain network that can confirm transactions in near real time. Currently, the ethereum blockchain network block is 12 seconds, and clients usually wait for a couple of minutes before confirming a transaction.
2) *Permissioned:* They want the blockchain to be permissioned. Permissioning itself means various different things. Permissioning can include taking permission to join the network, it can include taking permission to be able create blocks; it can be taking permission to be able to send specific transactions and so on.
3) *Security:* Private networks as there are a limited number of participants, therefore, aren't enough hash power produced to make it secure. So, there is a need for consensus protocol that can keep the blockchain secure and immutable.
4) *Privacy:* Although the network is private, there is still a need for privacy in the network itself.
5) *Identity Privacy:* Identity privacy is the act of making the identity untraceable. The solution we saw earlier to gain identity privacy was to use multiple ethereum account addresses. But if multiple ethereum accounts are used, then smart contracts will fail ownership validation as there is no way to know whether all of these accounts actually belong to the same user.
6) *Data privacy:* Sometimes, we don't want the data to be visible to all the nodes in the network, but to specific nodes only.

Fig 1: Big Data Challenges



Now a day's big data facing many challenges like Infrastructure security, Data management, Data privacy and Integrity and reactive security. Many researchers are working on these challenges but still we have some conflicts.

II. PROPOSED SYSTEM

Blockchain is essentially based on peer to peer network, private key cryptography and blockchain protocols, where different technologies like distributed data storage, consensus mechanism and symmetric encryption algorithm are used. In our design we aim to make the system flexible so that it can enable the deployment of both transactions and smart contract into any blockchain system.

1) Transactions: The transaction is a signature on trade information in the Bitcoin system, which mainly consists of addresses of sender/receiver and transferred value.it will be added to the blockchain after all the nodes successfully verified the signature.

2) There records in the blockchain cannot modify unless one can control at least 51% of the nodes. In this model, instructions like querying, storing, and operating data are carried by transactions.

3) The smart contract in blockchain consists of contract address, private storage, and predefined functions. It is a computer program that runs automatically to transfer money or anything having value when a specific policy is met.

4) In order to trigger the contract smoothly each contract has its special own address. System applies the smart contract to manage the public key info data.

Algorithm

a) Function name and invoked arguments

b) Setting up functions: --- > address DM;
--- > structure PK;
Public key:
Unit 256[2] n;
Int Expiry time;
Byte 32 ID;

c) Function Public key()
DM= message.sender;
Len=0;
Return 1;

d) Function update Public key(n,ExT,ID)
If (DM = = message. Sender) then
If Exist (PK[i].n==n) then
PK[i].n=n;
PK[i].ExT=ExT;
PK[i].ID=ID;
Return 1;

e) Function queryPK(n)

f) If Exist[PK[i].n==n && PK[i].ExT)

g) Return 1;

h) Else return 0;

i) Function revoke PK(n, ID)

j) If (message.sender == DM) then
If Exist (PK [i}.n==n) then
Delete (PK[i]);
Len - -;

k) Return 1;

l) Else return 0;

Output: we analyse the table data gas cost of smart contract price values.

The main intention is to analyse the big dataset and identify attribute values, observe the values changes and also identify the price changes in dynamically with certain variations. Take sample dataset for preliminary research as gas cost prediction and taken as useful inputs for consideration.

Using encryption and decryption algorithm we get some hash values. In this manner we tried to analyse and computing the sample gas cost prediction data set for our evaluations. And use other related data sets for compare the results.

III. PERFORMANCE EVALUATION

Our intention is to analyse the big dataset and identify the values changes and also identify the price changes in dynamically. Take sample dataset for preliminary research as gas cost prediction and taken as useful inputs for consideration. Here we propose the algorithm for security purpose to maintain the stored data and processing environment also. Future work of the project is to provide strong security wall for distributed storage and processing.

Gas cost of smart contract: gas price=2 gwei, ether=402.14 USD

Operation	Gas Used	Actual cost	USD
Update	147806	0.000295612	0.11887741
Query	27334	0.000054668	0.02198419
Revoke	36334	0.000072668	0.02922271
Deploy	838800	0.001677600	0.67463006

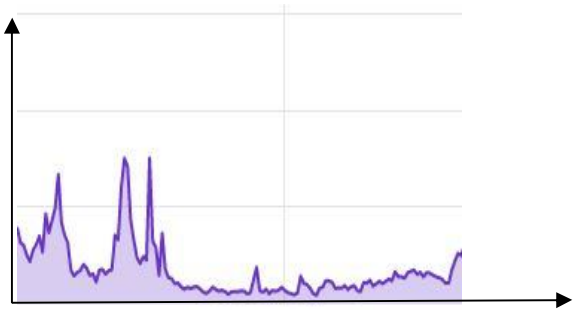


Fig2. Price value

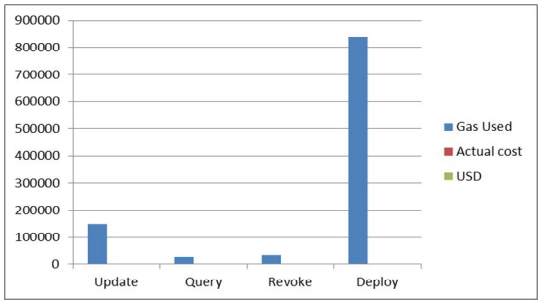


Fig 3. Graphical model

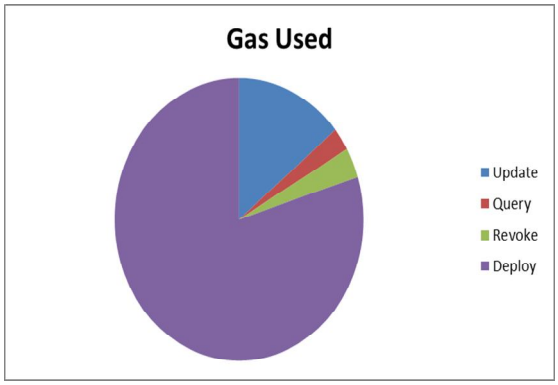


Fig 4. Gas used reprasentation

IV. CONCLUSION

We have proposed a blockchain-based secure and lightweight authentication for Cloud computing system. Our proposed system combines the blockchain and cryptographic algorithm to realize and establish a Secure and authentication system with the characteristics of decentralizing, privacy preserving. Besides, the security of the proposed scheme is analyzed. To provide Security for big data and cloud using high secure cryptographic algorithm. Here we propose the algorithm for security purpose to maintain the stored data environment. Future work of the project is to provide strong security wall for distributed storage and processing

V. ACKNOWLEDGMENT

The authors would like to express deep sense of appreciation and heartfelt thanks to the all the researcher of big data and cloud environment related journals, those journals are very helpful to gain knowledge on domain area, their untiring support and extended help in sharing the open access journals.

REFERENCES

[1] T. Issn-, "Privacy & Security in Healthcare Data in Cloud Storage using Blockchain," vol. 50, no. 7, pp. 1–8.
[2] P. K. Kalangi, "Efficient Secure Authentication Protocol for 5G Enabled Internet of Things Network," vol. 10, no. June, 2020.
[3] B. P. Goud, S. S. Reddy, and K. P. Kumar, "Smart Attendance Notification System using SMTP with Face Recognition," Int. J. Innov. Technol. Explor. Eng., vol. 9, no. 5, pp. 337–342, 2020, doi: 10.35940/ijitee.d1506.039520.
[4] K. P. Kumar and T. S. Durga, "Security Analysis Using Handover Strategies for Multi-Homed Body Sensor Networks," Asian J. Comput. Sci. Inf. Technol., vol. 1, no. 4, pp. 2011–2014, 2013.
[5] K. P. Kumar, T. N. S. Padma, and B. P. R. Goud, "Automatic Text Summarization Using LSTM Based On Sentence Semantics," vol. 8, no. 6, pp. 197–203, 2020. International Journal of All Research Education and Scientific Methods (IJARESM), ISSN: 2455- 6211
[6] Gartner Inc. More than half of major new business processes and systems will incorporate some element of the internet of things. Technical Report, 2016
[7] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. Computer networks, 54(15):2787–2805, 2010.
[8] Badis Hammi, Rida Khatoun, Sherali Zeadally, Achraf Fayad, and Lyes Khoukhi. IoT Technologies for smart cities. IET Networks, 7(1):1–13, 2018.
[9] Martin Wollschlaeger, Thilo Sauter, and Juergen Jasperneite. The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0. IEEE industrial electronics magazine, 11(1):17–27, 2017.
[10] Jha A, Dave M. and Madan, S. 2016. A Review on the Study and Analysis of Big Data using Data Mining Techniques, International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol6, Issue 3.

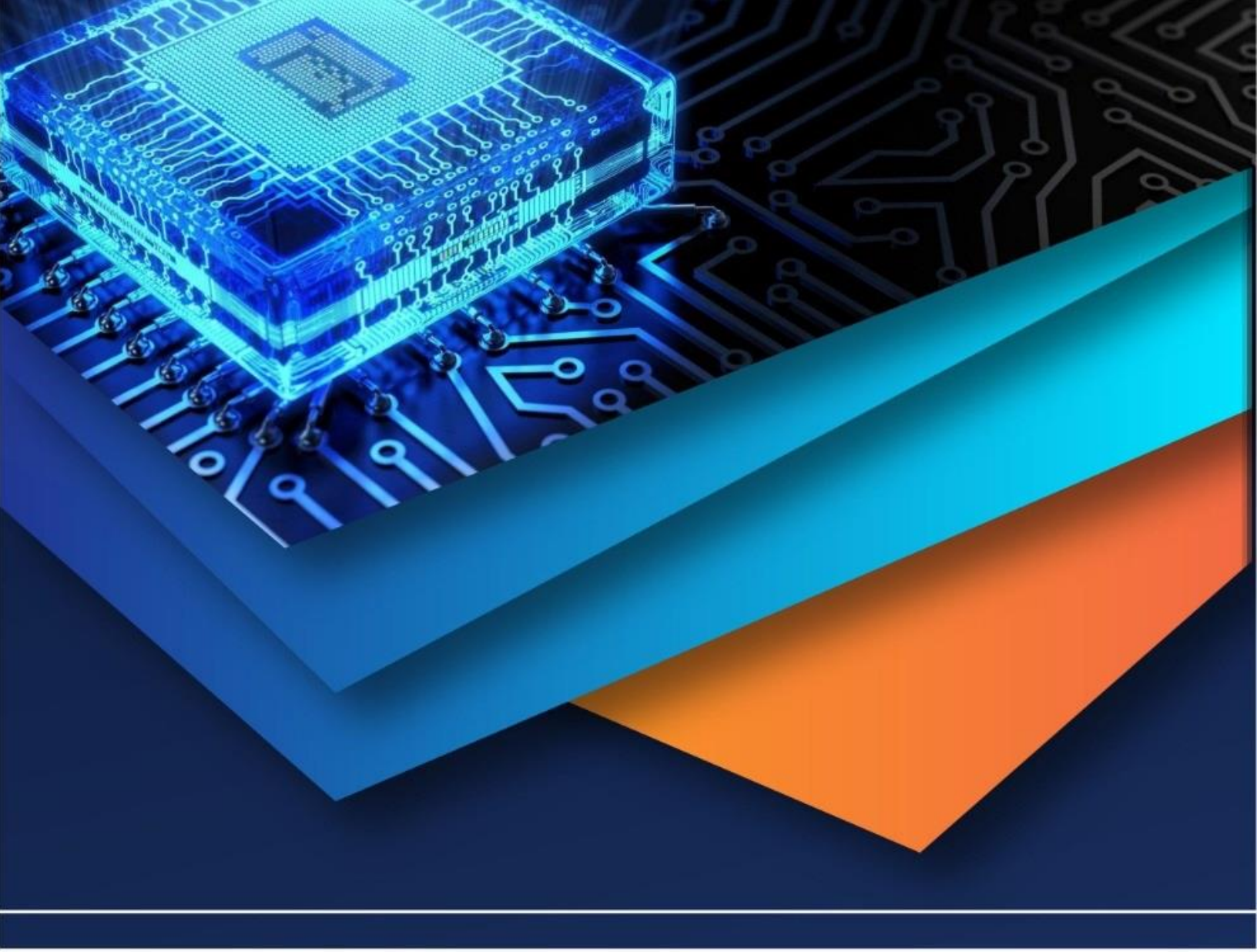
AUTHORS DETAILS

First Author – K Praveen Kumar
Assistant Professor
Department of Information Technology
Anurag University Hyderabad
Email id: praveenit@cvsr.ac.in
https://orcid.org/**0000-0002-8378-4191**

Second Author – T N S Padma
Assistant Professor
Department of Information Technology
Sreenidhi Institute of Science and Technology Hyderabad
Email id: padmathandu@sreenidhi.edu.in

Third Author – B Ravi Raju
Assistant Professor
Department of Information Technology
Anurag University, Hyderabad
Email id: ravirajubit@cvsr.ac.in

Fourth Author – B Pruthvi raj Goud
Assistant Professor
Department of Information Technology
Anurag University, Hyderabad
Email id: pruthvirajit@cvsr.ac.in



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY