GOVERNMENT FUND DISTRIBUTION AND TRACKING SYSTEM USING BLOCKCHAIN TECHNOLOGY

SAHIL SIDDHARTH JAMBHULKAR
Research Scholar, Department of Electronics and Telecommunication, Pune Institute of Computer Technology, Pune,

VISHAKHA PRASHANT RATNAPARKHI
Research Scholar, Department of Computer Engineering, Pune Institute of Computer Technology, Pune.

Abstract- Governments need to cater to a huge number of responsibilities of a state. The working of state governments involves huge number of transactions towards various operations that need to be carried out throughout the state. This includes new projects, repair and maintenance works, awarding contracts, paying of government employees, farmer schemes and so on. A major hurdle that the top government face is the low level corruption that is sometimes impossible to track which deprives the state progress. Tracking it is a very difficult task due to the current system. Here we propose a smart system to track funds allocated to the state government as they travel through the government process at each stage. We here make use of blockchain technology to secure the transactions at every stage while maintaining transparency in every transaction sealing every transaction with proofs as the funds move ahead. Blockchain, originally block chain, is a growing list of records, called blocks that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. In this project researcher use Blockchain Algorithms for security like AES for Encryption and Decryption By design, a blockchain is resistant to modification of the data. In this paper we propose a system to track funds allocated to the government as they travel through the government process at each stage using Key pair generation algorithm, Metadata file decryption and Data verification algorithms. This system uses block-chain technology to maintain the transparency & security at every stage as the funds move ahead. This system allows us to maintain the crystal clear record with all users who are connected in the chain to transaction the data on a need to know basis. The system makes use of encryption to secure transactional data using hash values to maintain a block of transactions in a chain manner, which is maintained & verified by every node involved to verify the transaction and save the data in a transparent form within the government. The system allows for a full proof, secure & authentic fund allocation & fund tracking system help to form an incorruptible government procedure.

Keywords— Blockchain, Security, Transparency, Encryption, Government Funds, Cryptography, AES.

I. INTRODUCTION

Blockchain is touted for its capability to improve the trust and straightforwardness of information based exchanges among people and associations. The innovation offers guarantee when deliberately applied in the correct settings. Customarily, associations working their own, singular IT frameworks trying to team up must deal with difficulties including compromise of data, recognizing a solitary wellspring of truth, and encouraging responsibility. Blockchain innovation tends to these difficulties by giving a specialized establishment that underpins the execution of shared business forms such that no single substance controls the whole framework. Government has a characteristic need to assemble, support, and ensure open trust in data and frameworks. In certain circumstances, blockchain may help improve this trust.

1.1 Background and Motivation

Customary social database the board arrangements (for example Prophet and SQL), sent universally across a huge number of uses, have one significant operational imperative – the administration of information is performed by a couple of substances who must be trusted. Disseminated Ledger Technologies (DLT, normally alluded to as blockchain), an option compositional way to deal with overseeing information, and evacuates the requirement for a confided in power to store and offer an unendingly developing arrangement of information. A basic attribute of a blockchain is trust. Blockchain have advanced marks and use keys to approve and check exchanges and emphatically recognize the initiator. When recorded to the chain, a blockchain record can't be erased or controlled. New squares may just be attached to the chain, guaranteeing information trustworthiness and making an unquestionable review trail where the mutual record gives perceivability to all members, at the same time. Moreover, information components can be independently permissioned, so members see just fitting exchanges. Applications oversaw by a solitary substance would ordinarily not advantage from utilizing blockchain innovation. As the name connotes, blockchain is a chain of squares. Each square speaks to a record or set of information, that is connected to others with cryptography. Each square contains some open data to give open information about the activity, time, or some other component of the record, making an open transcript of how the data creates, known as a "record." As exchanges enter a blockchain framework, an accord model is utilized to figure out which next arrangement of substantial exchanges, or square, ought to be annexed to the record. Since accord is built up over a disseminated organize for hubs, there is no focal position that administers the approval and consideration of new exchange information. As most blockchain programming is open source, the principles that settle the squares and included exchange information are accessible for survey. For open blockchain frameworks, the information itself is accessible for direct perception by any individual who cares to get to it. This makes open blockchain datasets saw of as increasingly solid to a greater number of clients.

1.2 Motivation

Usually when a project is allocated funds, there is no knowledge as to how these funds are being used and a large part of it is never show in records due to corruption. To solve this problem, a system has been proposed using Blockchain to provide the transparency.

1 A major hurdle that the top government faces is the low-level corruption that is sometimes impossible to track which deprives the state progress.

2 Blockchain technology is an upcoming technology and said to be one of the most promising technologies which would revolutionize the world.

1.3 Problem Statement

Governments need to cater to a huge number of responsibilities of a state. The working of state governments involves huge number of transactions towards various operations that need to be carried out throughout the state. This includes new projects, repair and maintenance works, awarding contracts, paying of government employees, farmer schemes and so on. A major obstacle that the top government face is the low level corruption that is sometimes not possible to track which deprives the state progress. Tracking it is a very complicated task due to the current system. But in proposed system we overcome this drawbacks by using block chain approach. We here make use of blockchain technology to secure the transactions at every stage while maintaining transparency in every transaction sealing every transaction with proofs as the funds move ahead. Blockchain, originally block chain, is a growing list of records, called blocks that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. In this project researcher use Blockchain Algorithms for security like AES for Encryption and Decryption By design, a blockchain is resistant to modification of the data. In this paper we propose a system to track funds allocated to the government as they travel through the government process at each stage using Key pair generation algorithm, Metadata file decryption and Data verification algorithms.

II. REVIEW OF LITERATURE

Literature survey is the most important step in any kind of research. Before start developing we need to study the previous papers of our domain which we are working and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers. In this section, we briefly review the related work on Government Fund Tracking System using Block-chain Technology.

In this paper, the author propose an imaginative blockchain-based IOT engineering to help fabricate an increasingly secure and solid IOT framework. By examining the deficiencies of the current IOT design and the benefits of the Block-chain innovation. We decay and redesign the first IOT design to shape another, multi-focus, incompletely decentralized engineering. Accordingly, the proposed engineering speaks to a huge improvement of the first design, which gives another heading to the IOT advancement.[1]

This paper provides, through its technique, an itemized examination of the square chain fit in the inventory network industry. It characterizes the particular components of square chain that influence store network, for example, versatility, execution, agreement instrument, security contemplations, area proof and cost.[2]

Data mining system for anticipation and discovery of fiscal report extortion right now. These instructive factors are being use for executing affiliation rule digging for anticipation and three prescient mining strategies in particular K-implies, Multi-Level Feed Forward Network, Genetic programming for discovery of budgetary misrepresentation. This exploration can forestall false monetary revealing and distinguish it if the executives of the association is fit for executing budget summary misrepresentation in spite of the nearness of against extortion condition. [3]

Data mining structure for evasion and uncovering of fiscal summary extortion right now. The structure utilized right now the ordinary progression of information mining. These valuable factors are being utilized for actualizing affiliation rule digging for counteraction and three prescient mining procedures in particular K-implies, Multi-Level Feed Forward Network, Genetic programming for identification of money related misrepresentation.[4]

In this paper, the author propose a square chain empower efficient information assortment and secure sharing plan consolidating Ethereal square chain and profound support learning (DRL) to make a solid and safe condition. Right now, is utilized to achieve the most elevated measure of gathered information, &the square chain innovation is utilized to ensure wellbeing and unwavering quality of information sharing.[5]

Blockchain is portrayed by its decentralized nature, respectability of the information put away in the chain and its receptiveness. Because of these qualities, somewhere else where Blockchain can be utilized is to discharge government assets for an undertaking. Normally when an undertaking is allotted assets, there is no information with respect to how these assets are being utilized and a huge piece of it is never appeared in records because of debasement. To take care of this issue, a framework has been proposed utilizing Blockchain to give the straightforwardness.[6]

In this paper, a general versatile fuzzy control plot through yield following mistake input has been proposed for handy yield following of a class of questionable nonlinear frameworks with unmeasurable states and totally obscure elements including parametric or potentially auxiliary vulnerabilities and outer unsettling influences. The proposed conspire gives an integral asset to target following of unmanned vehicles, rockets, versatile robots, and so forth., at whatever point just following blunder (inconsistency) can be accessible. [7]

This paper portrays a strategy for consolidating client information with naturally created rules. The presentation improved outcomes yet in general the improvement was not critical, this might be a result of the techniques that were tried. Another perception that is produced using these outcomes is that despite the fact that there was some variety in the exhibition as for restores, the hazard balanced execution was considerably more stable.[8]

In this paper, we propose an item recognizability framework dependent on blockchain innovation, in which all item moving chronicles are interminably recorded in an appropriated record by utilizing shrewd agreements and a chain is shaped that can follow back to the wellspring of the items. Our framework has evident decentralized attributes, which fundamentally lessens the chance of secretly altering information inside endeavors. Our framework is described by information availability, sealing, and protection from man-in-the-middle attacks. [9]

This paper proposed another data sharing plan dependent on blockchain innovation. Clients can deal with their information and comprehend the information being gathered about them and how to utilize it without confiding in any outsider. Nonetheless, the plan didn't consider the chance of the endeavor itself messing with information. [10]

III. PROPOSED SYSTEM ARCHITECTURE

The proposed system is used to track the funds allocated to the state government as they travel through the government process at every stage. We here make use of block-chain technology to secure the transactions at each stage while maintaining transparency in every transaction sealing every transaction with proofs as the funds move ahead. This allows maintaining crystal clear record with on-demand right to transactional data on a need to know basis. The system makes use of encryption to secure transactional data by means of hashes to maintain a block of transactions in a chain manner which is maintained and verified by every node involved to authenticate the transaction & save the data in transparent form within the government. The system allows for a full proof, secure & authentic fund allocation and fund tracking system to help form an incorruptible government process.

In this we are using 2 modules i.e. User and Admin.

1. **Module 1** - Government: - Government will give the fund which is requested by the user.
2. **Module 2** – Authority (TPA):- This will authorize or verify the user that it is a valid user as well as valid request or not.
3. **Module 3** - User (Customer):- User will request for the fund according to their needs.

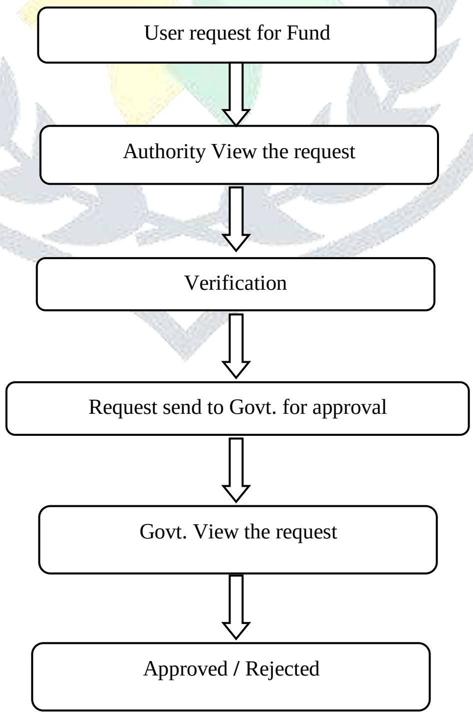

Fig.1 Flow Diagram of System

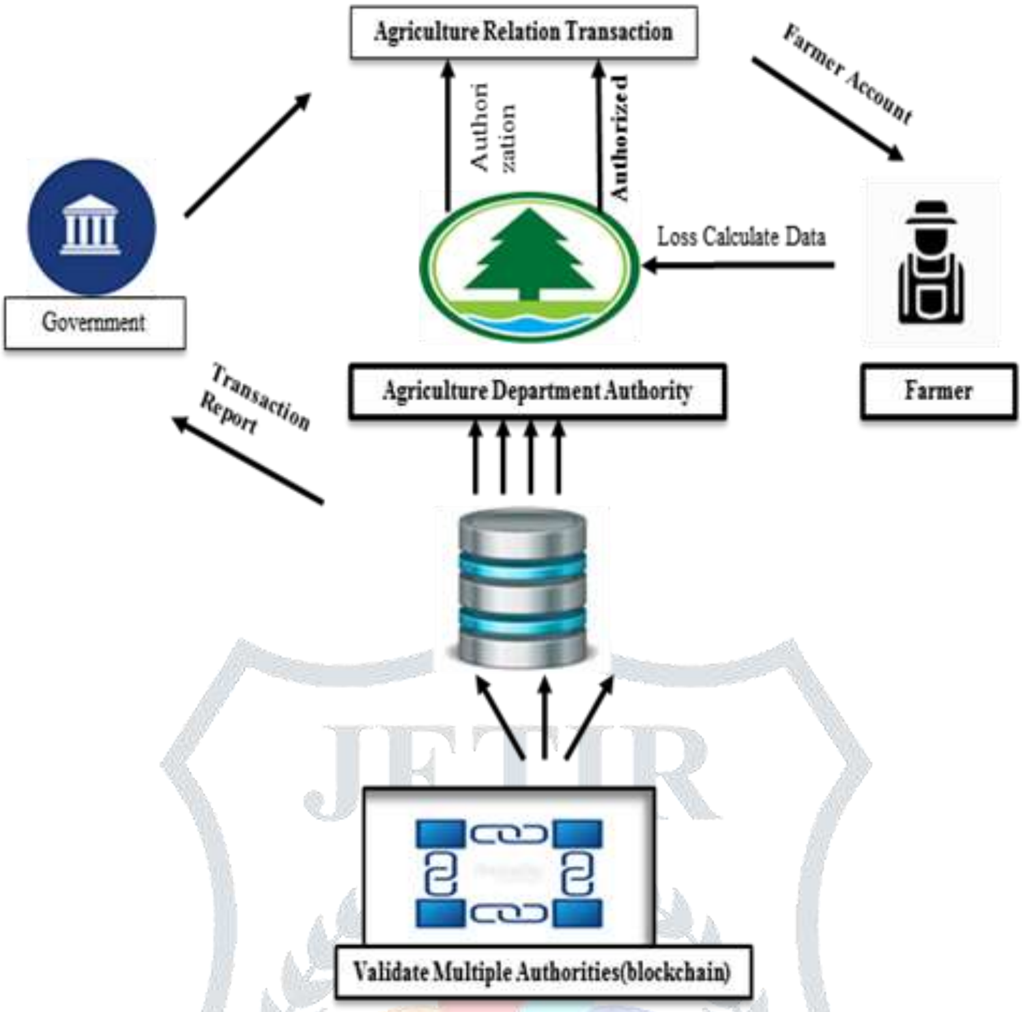

Fig.2 Proposed System Architecture

IV. ALGORITHM DETAILS

4.1 AES with Key generation Phase:

AES with SHA Key: For encrypting metadata file we are using AES encryption algorithm. The encryption process generates a symmetric key called around a key. SHA-1 is applied on this key which creates block of data which is hold by an array of data called the state array. The method can create 128/192/256-bit keys.

Algorithm: Blockchain Based Keypair generation algorithm
Data : userKey
Result : SecretKeySpec secreteKey
1. byte[] key= userKey.getBytes("UTF-8"); 2. MessageDigest sha = MessageDigest.getInstance("SHA-1"); 3. key = sha.digest(key); 4. key = Arrays.copyOf(key, 16); 5. SecretKeySpec secretKey = new SecretKeySpec(key,"AES") 6. **return** secreteKey;

4.2 Decryption:

In Method follows a process which is before reconstructing the File joiner needs the sequence of chunks in which they are being joined. This sequence information is stored in a metadata file which is being encrypted before storing it in the cloud. So the decryption module decrypts the metadata file for file joiner

Algorithm: Metadata file decryption
Data: Ciphertext CT, Cipher key CK
Result: File F
1. setKey(CK); 2. CipherTransform Secure Cipher CipherTransform.getInstanc ("AES/ECB/PKCS5Padding"); 3. SecureCipher.init (CipherTransform.DECRYPT_MODE, CK); 4. F = SecureCipher.doFinal (Base64.getDecoder().decode(CT) 5. **return** F

4.3 TPA Process:

The system has three main models which are involved. Cloud users, cloud storage and third-party auditor are the part of it. Cloud storage and cloud service provider are the same in this system. Cloud users stored the data over the cloud by registering to a particular cloud storage provider. Data owner's stored' data on cloud storage space. The public cloud service provider is only responsible for storing data and is not responsible for any damage of data to give a proof of the integrity of the stored user's data. The system uses TPA for the process of auditing. TPA is nothing but an analyser which verifies the data integrity on behalf of users in the system and minimizes the overload of the user. To have successful TPA Following security and performance challenges should be achieved

1) Efficiency: While data uploading and auditing of data, data transfer, communication and computation cost must be low.
2) Storage accuracy: TPA should complete the auditing task and pass it without data on that side or damaging stored data.
3) Privacy-preserving: TPA should not exploit data of users while collecting for the process of auditing.
4) Prohibit Attacks: -To ensure that the frame and collude attack should not take place

Algorithm: Data verification
Data: File F, Public key PuK, Users Digital Signature UDigSign
Result: Verified result R
1. Signature dSign = Signature.getInstance(MD5withRSA); 2. dSig.initVerify(PuK); 3. dSig.update(F.getBytes()); 4. R=dSig.verify(UDigSign); 5. **return** R;

V. MATHEMATICAL MODELLING

5.1 Scheme Details.

1. Let G1, G2 and GT be multiplicative cyclic groups of prime order p, and e : G1 × G2 → GT be a bilinear map as introduced in preliminaries. Let g be a generator of G2.
2. H(£) is a secure map-topoint hash function: {0, 1}∗ → G1, which maps strings uniformly to G1. Another hash function h(·) : GT → Zp maps group element of GT uniformly to Zp.

5.2 Setup Phase:

1. The cloud user runs KeyGen to generate the public and secret parameters. Specifically, the user chooses a random signing key pair (spk, ssk), a random x ← Zp, a random element u ← G1, and computes v ← gx. The secret parameter is sk = (x, ssk) and the public parameters are pk = (spk, v, g, u, e(u, v)).
2. Given a data file F = (m1, . . . ,mn), the user runs SigGen to compute authenticator µi for each block mi: µi ← (H(Wi) · umi)x ∈ G1.

3. Here Wi = name||I and name is chosen by the user uniformly at random from Zp as the identifier of file F. Denote the set of authenticators by ∑= {µi}1≤i≤n.
4. The last part of SigGen is for ensuring the integrity of the unique file identifier name.
5. One simple way to do this is to compute t = name||SSigssk(name) as the file tag for F, where SSigssk(name) is the signature on name under the private key ssk.
6. For simplicity, we assume the TPA knows the number of blocks n.

5.3 Audit Phase:

1. The TPA first retrieves the file tag t. With respect to the mechanism we describe in the Setup phase, the TPA verifies the signature SSigssk(name) via spk, and quits by emitting FALSE if the verification fails.
2. Otherwise, the TPA recovers name. Now it comes to the "core" part of the auditing process. To generate the challenge message for the audit "chal", the TPA picks a random c-element subset I = {s1, . . . , sc} of set [1, n]. For each element i ∈ I, the TPA also chooses a random value _i (of bit length that can be shorter than |p|, as explained in [13]).
3. The message "chal" specifies the positions of the blocks that are required to be checked. The TPA sends chal = {(i, £i)}i∈I to the server. Upon receiving challenge chal = {(i, µi)}i∈I , the server runs GenProof to generate a response proof of data storage correctness.
4. Specifically, the server chooses a random element r ← Zp, and calculates R = e(u, v)r ∈ GT . Let µ′ denote the linear combination of sampled blocks specified in chal: µ′ = Pi∈I £imi.
5. To blind µ′ with r, the server computes: µ = r+µ′ mod p, where = h(R) ∈ Zp.
6. Meanwhile, the server also calculates an aggregated authenticator ∑ = Qi∈I µ i ∈ G1. It then sends {µ, £,R} as the response proof of storage correctness to the TPA.
7. With the response from the server, the TPA runs VerifyProof to validate the response by first computing = h(R) and then checking the verification equation

5.4 Security Analysis

1. We evaluate the security of the proposed scheme by analyzing its fulfillment of the security guarantee described, namely, the storage correctness and privacy-preserving property.
2. We start from the single user case, where our main result is originated. Then we show the security guarantee of batch auditing for the TPA in multi-user setting.
3. We need to prove that the cloud server cannot generate valid response for the TPA without faithfully storing the data, as captured by Theorem 1.
4. Theorem 1: If the cloud server passes the Audit phase, then it must indeed possess the specified data intact as it is.
5. Proof: The proof consists of two steps. First, we show that there exists an extractor of µ′ in the random oracle model. Once a valid response {£, µ′} are obtained, the correctness of this statement follows from
6. Now, the cloud server is treated as an adversary. The extractor controls the random oracle h(£) and answers the hash query issued by the cloud server.
7. For a challenge £ = h(R) returned by the extractor, the cloud server outputs {£, µ,R} such that the following equation holds.

VI. RESULT ANALYSIS

Researcher now assess the performance of the proposed privacy-preserving public auditing schemes to show that they are indeed lightweight. We will focus on the cost of the efficiency of the privacy-preserving protocol and our proposed batch auditing technique. The experiment is conducted using C on a Linux system with an Intel Core 2 processor running at 1.86 GHz, 2048 MB of RAM, and a 7200 RPM Western Digital 250 GB Serial ATA drive with an 8 MB buffer. Security is provided while storing the data using a chunk generation algorithm and verification of chunks using lightweight Third Party Auditor (TPA). TPA uses digital signatures to verify user's data that are generated by RSA with MD5 algorithms.

6.1 Results

Results 1: Shows file size on x axis and Encryption Time on Y-axis

In this subsection, our System evaluates the performance of the proposed scheme by several experiments. System runs these experiments on a window machine with an Intel processor 2.30GHz processor and 8GB memory. All these experiments use Java programming language with the various encryption algorithms such as AES (Proposed system), CP-ABE (Existing System).

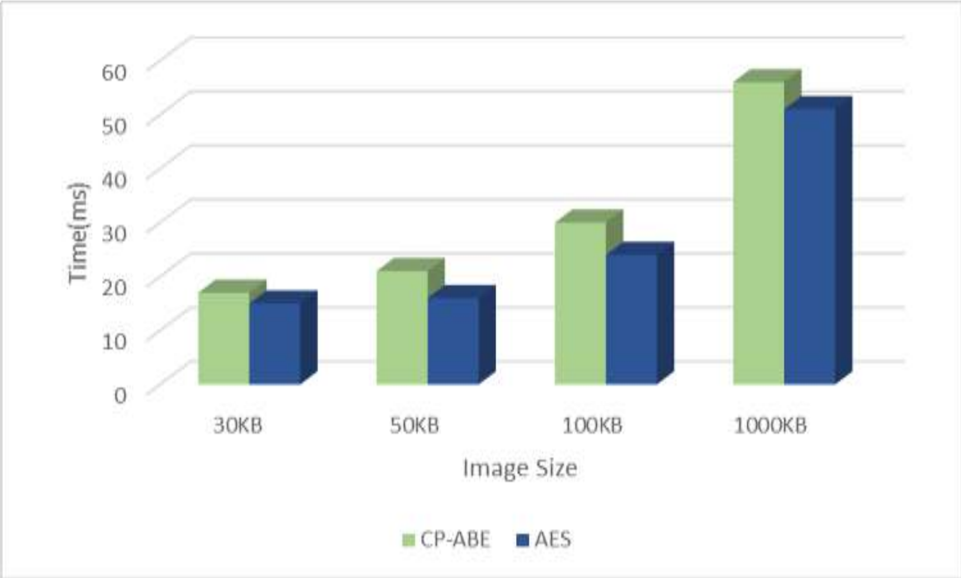

Fig 03: Shows file size on x axis and Encryption Time on Y-axis

Table 1: Show File Size and Encryption Time

Index Number	File size (KB)	ABE Encryption Time	AES Encryption Time
1	30	31	28
2	50	36	31
3	100	63	58
4	1000	102	93

Results 2: Shows file size on x axis and Decryption Time on Y-axis

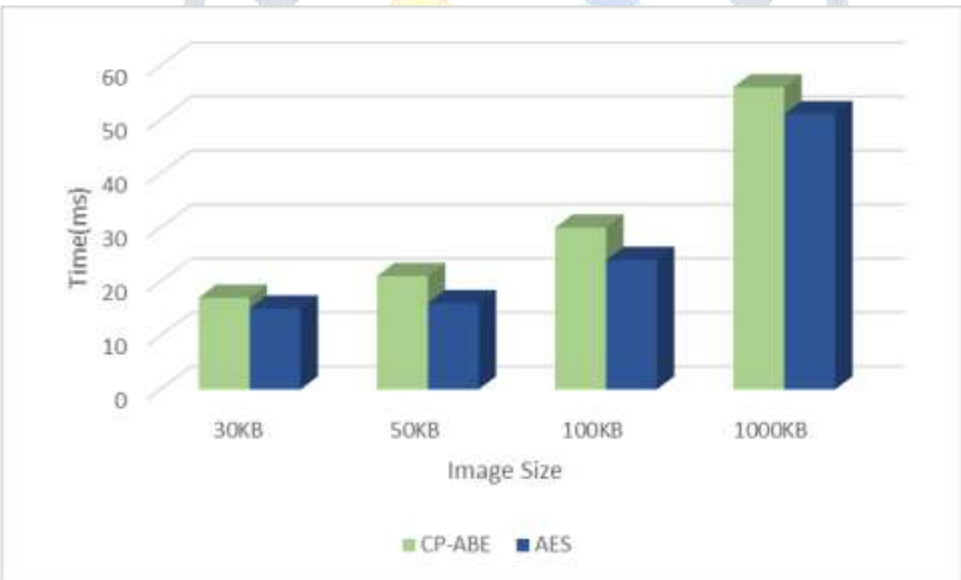

Fig 04: Shows file size on x axis and Decryption Time on Y-axis

Table 2: Show File Size and Decryption Time

Index Number	File size (KB)	ABE Decryption Time	AES Decryption Time
1	30	12	9
2	50	16	12
3	100	26	21
4	1000	52	46

Results 3: Shows file size on x axis and Uploading Time on Y-axis

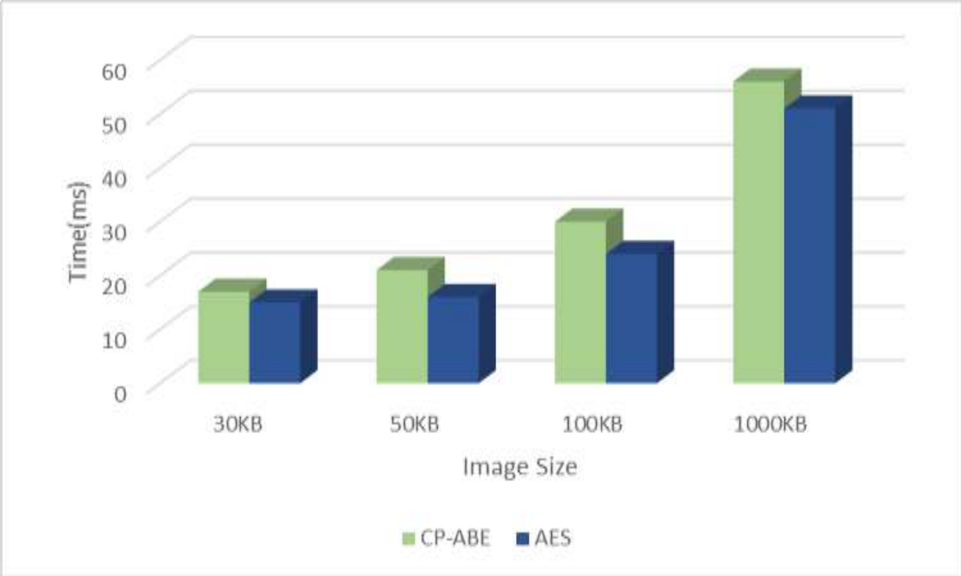

Fig 05: Shows file size on x axis and Uploading Time on Y-axis

Table 3: Show File Size and Uploading Time

Index Number	File size (KB)	ABE uploading Time	AES uploading Time
1	30	36	32
2	50	42	35
3	100	69	62
4	1000	111	96

Results 4: Shows file size on x axis and Downloading Time on Y-axis

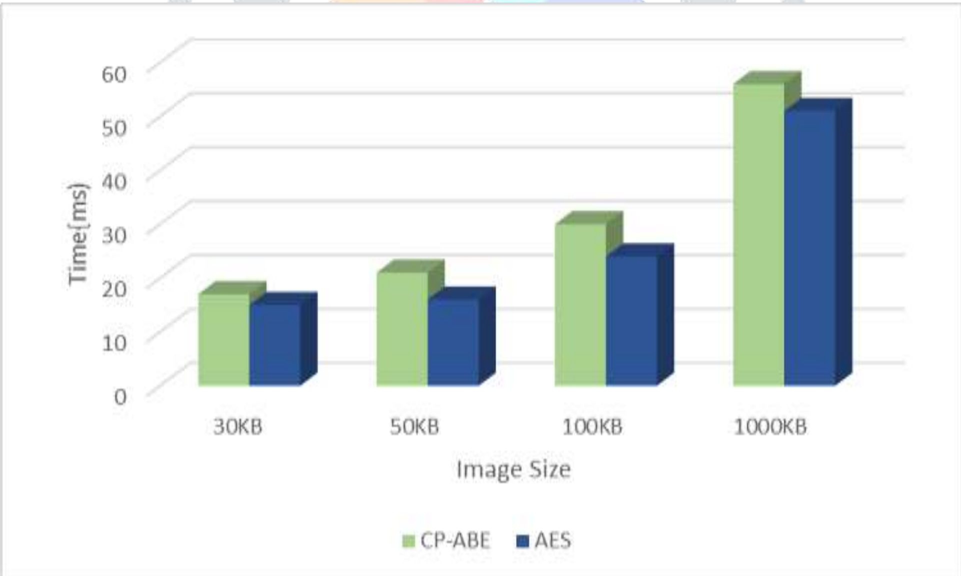

Fig 06: Shows file size on x axis and Downloading Time on Y-axis

Table 4: Show File Size and Downloading Time

Index Number	File size (KB)	ABE Downloading Time	AES Downloading Time
1	30	17	15
2	50	21	16
3	100	30	24
4	1000	56	91

CONCLUSION

In this paper, researcher considered about the blockchain applications, we even have to consider the access and privacy challenges though. This allows to maintain crystal clear record with on demand right to transactional data on a need to know basis. The system makes use of encryption to secure transactional data using hashes to maintain a block of transactions in a chain manner which is maintained and verified by every node involved to verify the transaction and save the data in a transparent form within the government. The system allows for a full proof, secure and authentic fund allocation and fund tracking system to help form an incorruptible government process. Even then, with further enhancements, this blockchain model can provide a transparency in all the government transactions. There will be no discrepancies of any kind. Because of the decentralized ledger all the transactions can be verified and cannot be altered. The money that is released can be tracked, anyone and everyone can find out how the money is being used. Such a blockchain will surely reduce the ongoing corruption It will create a huge impact on the economic development of a country.

REFERENCES

[1] Jiafu Wan, Jiapeng Li, Muhammad Imran, Di Li, Fazal-e-Amin, "A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory",IEEE Transactions on Industrial Informatics Volume: 15 , June 2019.

[2] Antonios Litke, Dimosthenis Anagnostopoulos, Theodora Varvarigou, "Blockchains for Supply Chain Management: Architectural Elements and Challenges towards a Global Scale Deployment", MDPI January 2019.

[3] Mrs. R.Meenatkshi , Mrs. K.Sivaranjani, "A Comparative Study on Fraud Detection in Financial Statement utilizing Data Mining Technique", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.7, July-2016, pg. 382-386.

[4] Analysis KK Tangod, GH Kulkarni, "Discovery of Financial Statement Fraud utilizing Data Mining Technique and Performance", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015 .

[5] Chi Harold Liu, Senior Member, IEEE, Qiuxia Lin, Shilin Wen. "Blockchain-empowered Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning", IEEE Transaction on Industrial Volume: 15, Issue: 6 , June 2019

[6] Apoorva Mohite, Ajay Acharya, "Blockchain for government support following utilizing Hyperledger", IEEE Transactions on Fuzzy Systems, April 2018

[7] Ning Wang, Jing-Chao Sun, Meng JooEr,"Tracking-Error-Based Universal Adaptive Fuzzy Control for Output Tracking of Nonlinear System with Completely Unknown Dynamics" ,IEEEAPRIL 2017.

[8] Adam Ghandar, Zbigniew Michalewicz, Ralf Zurbruegg, Chee Cheong, "Record Tracking Fund Enhancement Using Evolving Multi-Criteria Fuzzy Decision Models",IEEE Congress on Evolutionary Computation.

[9] Shangping Wang, Dongyi Li, Yaling Zhang, Juanjuan Chen, "Savvy Contract-Based Product Traceability System in the Supply Chain Scenario", IEEE Access, 2019.

[10] M. Kim, B. Hilton, Z. Burks, and J. Reyes, "Coordinating Blockchain, Smart Contract-Tokens, and IoT to Design a Food Traceability Solution," in ninth IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Univ British Columbia, Vancouver, Canada, Nov. 2018.

[11] Fouad KheliÞ(2018)[11], Secure and Privacy-preserving Data Sharing in the Cloud based on Lossless Image Coding, Preprint submitted to Signal Processing February 13, 2018 DOI: 10.1016/j.sigpro.2018.02.016

[12] Ranjeet Kumar(2019)[12], An efficient technique for image compression and quality retrieval using matrix completion, Journal of King Saud University – Computer and Information Sciences xxx (xxxx) xxx journal homepage: www.sciencedirect.com https://doi.org/10.1016/j.jksuci.2019.08.002

[13] Mamta Meena(2016)[13], Hybrid Wavelet Based CBIR System using Software as a Service (SaaS) Model on public Cloud, 7th International Conference on Communication, Computing and Virtualization 2016, Procedia Computer Science 79 (2016) pp. 278 – 286, Available online at www.sciencedirect.com doi: 10.1016/j.procs.2016.03.036

[14] B. Nivedha(2017)[14], Lossless Image Compression In Cloud Computing, 2017 International Conference on Technical Advancements in Computers and Communications, 978-1-5090-4797-0/17 $31.00 © 2017 IEEE DOI 10.1109/ICTACC.2017.37

[15] J. Smith(2012)[15], Progressive encoding and compression of surfaces generated from point cloud data, Computers & Graphics 36 (2012) pp. 341–348, Contents lists available at SciVerse ScienceDirect journal homepage: www.elsevier.com/locate/cag http://dx.doi.org/10.1016/j.cag.2012.03.032

[16] Man-Wen Tian(2019)[16], Research on image recognition method of bank financing bill based on binary tree decision, J. Vis. Commun. Image R. 60 (2019) pp. 123–128 journal homepage: www.elsevier.com/ locate/ jvci https://doi.org/10.1016/j.jvcir.2018.12.016

[17] A.M. Vengadapurvaja (2017)[17], An Efficient Homomorphic Medical Image Encryption Algorithm For Cloud Storage Security, 7th International Conference on Advances in Computing & Communications, ICACC-2017, 22- 24 August 2017, Cochin, India Procedia Computer Science 115 (2017) pp. 643–650 Available online at www.sciencedirect.com 10.1016/j.procs.2017.09.150

[18] Chi Yang(2013)[18], A spatiotemporal compression based approach for efficient big data processing on cloud, Journal of Computer and System Sciences, DOI: 10.1016/j.jcss.2014.04.022 http://dx.doi.org/10.1016/j.jcss.2014.04.022

[19] Chaowei Yang(2016)[19], Utilizing Cloud Computing to address big geospatial data challenges, Computers, Environment and Urban Systems xxx (2016) xxx–xxx CEUS-01097; No of Pages 9, journal homepage: www.elsevier.com/locate/ceus http://dx.doi.org/10.1016/j.compenvurbsys.2016.10.010

[20] Farhan Israk Yen(2019)[20], Efficient Image Compression for Cloud System, 2019 International Conference on Sustainable Technologies for Industry 4.0 (STI), 24-25 December, 978-1-7281-6099-3/19/$31.00 ©2019 IEEE