IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed ( Group -I) Journal Volume 11, Iss 5, 2022

# BLOCKCHAIN-BASED AMPLIFICATION OF CLOUD SECURITY

Ms. Monika Dixit Bajpai
Asst. Professor, Dept of BCA, Institute of Management Studies, Noida

***Abstract:*** In the internet-dependent world, the demand for data is increasing day by day. This has generated an issue of massive data storage. To overcome this issue, a cloud-based storage service was developed. Today there is extensive involvement of cloud on business transactions and daily applications. This has raised the need to provide high end of security to the stored data; the project helps overcome this problem. The use of a blockchain network as an interface to access the data will help overcome the security of data on the cloud. The blockchain is a distributed public ledger and Internet-based computer network. The proposed system works on the ERP data of a company, on a private cloud, which is accessible through the internet from any place. It validates and secures the employee data of the company. Smartphone and laptop security features like biometrics and password validation can be to make this idea more robust and easier to use for end-user. The local validation process of laptops and smartphones acts as a user interface between the background and the user. This also acts as the next level of security for validation of user details. Thus, providing a more secure way of accessing the cloud service.

***Index Terms*** **– Cloud, Security, Blockchain, Data storage, internet.**

## I. INTRODUCTION

Recent years have witnessed the trend of increasingly relying on distributed infrastructures. This increased the number of reported incidents of security breaches compromising user's privacy, where third parties massively collect, process, and manage user's personal data. The aim of this proposed System is to provide a more comfortable and safer way to access the data on the cloud than the traditional System. Provide high end of security to the stored data. This allows the user to save data on the cloud without any worries. This will increase the trust of users to put high confidential data on the cloud, thus making the cloud technology safer and cheaper for all types of users. The system will remove the dependency of access of third-party companies to maintain the data on the cloud.

## II. LITERATURE SURVEY

Block-chain based data provenance can enable the transparency of data accountability in the cloud and help to enhance the privacy and availability of the provenance data. The system makes use of the cloud storage scenario and chooses the cloud file as a data unit to detect user operations for collecting provenance data. System design and implement Prov-Chain, an architecture to collect and verify cloud data provenance, by embedding the provenance data into blockchain transactions. Prov-Chain operates mainly in three phases:

1. provenance data collection.
2. provenance data storage.
3. provenance data validation.

Blockchain may be viewed as a public ledger, and each submitted dealings is placed during a list of blocks. This chain develops as new blocks are mounted to that incessantly. With an awfully designed data storage structure, transactions in Bitcoin system might occur with no third party, and therefore the core innovation to construct Bitcoin is blockchain, that was initially planned in 2008 and dead in 2009 [11].

The system presents eclipse attacks on the bitcoins peer-to-peer network. The attack allows an adversary controlling enough IP addresses to monopolize all connections to and from a victim bitcoin node. The attacker can further exploit the victim for attacks on bit-coins mining and consensus system, including double confirmation spending, selfish mining, and adversarial forks in the blockchain. The system takes a detailed look at the bitcoins peer-to-peer network, and quantify the resources involved in the attack via probabilistic analysis, Monte Carlo simulations, measurements, and experiments with live bit-coin nodes [4].

In standard centralized group action systems, every group action must be valid through the trustworthy central agency (e.g., the central bank), inevitably ensuing to the value and therefore the performance bottlenecks at the central servers. The distinction to the centralized model, the third party, is not any longer required in blockchain. Accord algorithms in blockchain are accustomed to maintaining information consistency in a distributed network. Bitcoin blockchain stores knowledge regarding user balances supported

ISSN PRINT 2319 1775 Online 2320 7876
Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 5, 2022

the unexpended dealings Output (UTXO) model. Any dealings must ask some previous unexpended transactions. Once this dealing is recorded into the blockchain, the state of these referred unexpended transactions switches from unexpended to spent. Therefore, transactions can be simply verified and tracked [12].

## I. OSED SYSTEM

The user request is verified and processed by the local System. This request is passed to the cloud server, which processes the request based on retrieval or upload of data on the cloud. In this process, the blockchain algorithm either encrypts or decrypts the data based on the request. Further, data integrity is checked by the cloud server. The output of the retrieval request is passed to the local server and displayed to the user. In the case of upload, after processing of the algorithm, the data appears on the cloud.

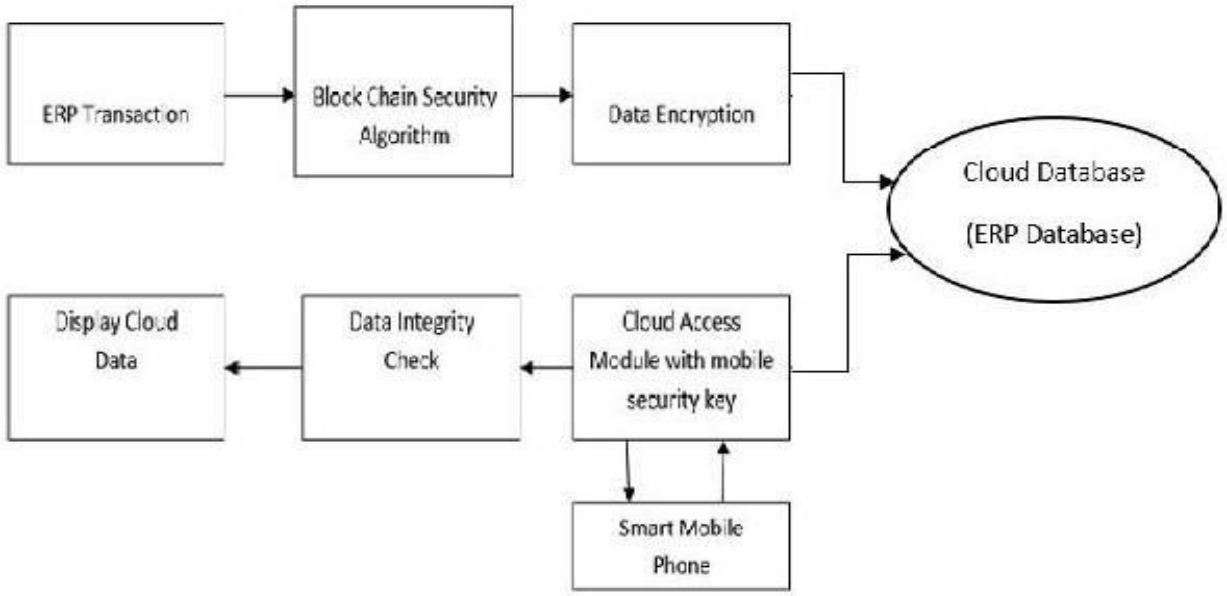


Figure 1. Working model of the proposed system.

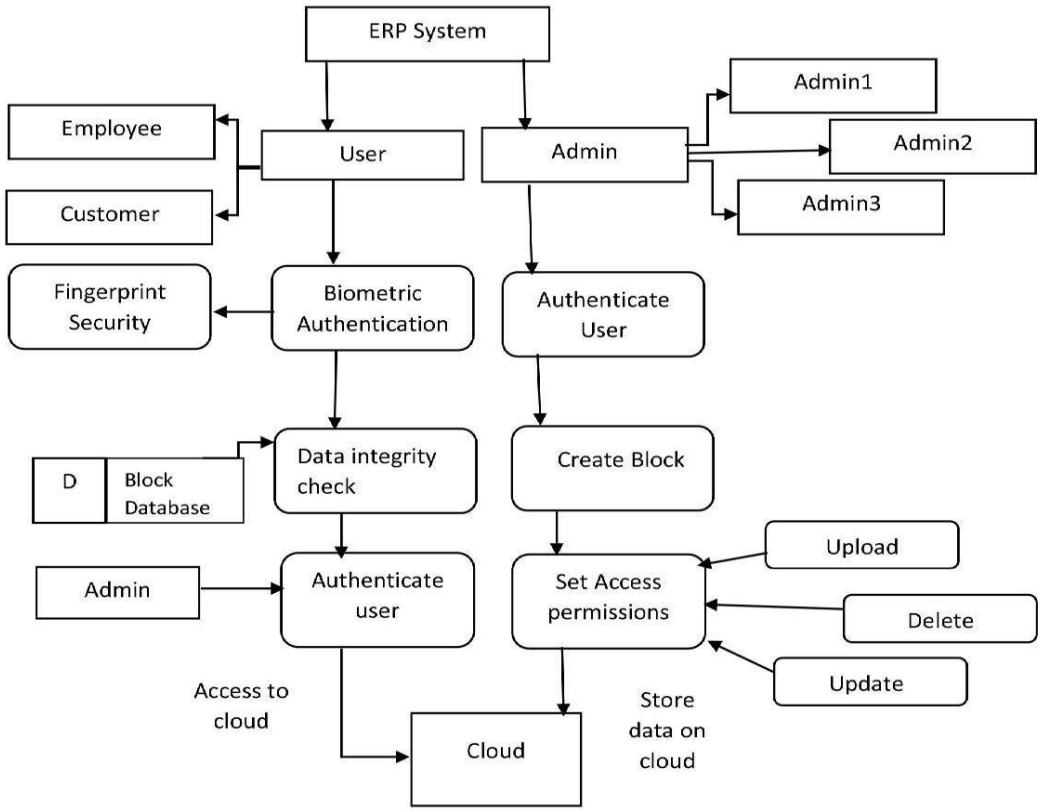


Figure 2. Data Flow for the proposed system.

ISSN PRINT 2319 1775 Online 2320 7876
Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 5, 2022

The System is dived into 4 modules: -
1. Server-side definition: connecting the user system with the cloud system.
2. Block-chain creation, verification, validation.
3. Android application:2 step verification system.
4. Cloud module: Data storage

## II. LS AND TECHNOLOGIES

### 4.1. AES Algorithm:

AES is a block cipher, meaning that encryption happens on fixed-length groups of bits. In our case, the algorithm defines 128-bit blocks. AES supports various key lengths of 128, 192 and 256 bits. Every block goes through many cycles of transformation rounds. The important part is that the key length does not affect the block size, but the number of repetitions of transformation rounds (the 128-bit key is ten cycles, 256 bit is 14). So AES will only encrypt 128 bit of data, but if the System wants to encrypt whole to a single ciphertext one can use GCM block mode.

– Confidentiality: The ability to prevent eavesdroppers from discovering the plaintext message, or information about the plaintext message.

– Integrity: The ability to prevent an active attacker from modifying the message without the legitimate users noticing.

– Authenticity: The ability to prove that a message was generated by a particular party and prevent forgery of new messages. This is usually provided via a Message Authentication Code (MAC). Note that authenticity automatically implies integrity.

AES with Galois/Counter Mode (GCM) block mode provides all those properties, and our System uses this block mode for encryption.

### 4.2. RSA Algorithm:

Hashing is the process of taking an input of any length and turning it into a cryptographic fixed output through a mathematical algorithm like RSA. The RSA algorithm can be used for both public-key encryption and digital signatures. Key Generation Algorithm-

1. Generate two large random primes, p and q, of an approximately equal size such that their product n=p*q is of the required bit length, e.g. 1024 bits.
2. Compute n=p*q and $\phi=(p-1)*(q-1)$.
3. Choose an integer e, $1<e<\phi$, such that $\gcd(e,\phi)=1$.
4. Compute the secret exponent d, $1<d<\phi$, such that $e*d\equiv 1 \bmod \phi$.
5. The public key is (n,e) and the private key (d,p,q). Keep all the values d, p, q and $\phi$ secret.
   - n is known as the modulus.
   - e is known as the public exponent or encryption exponent or just the exponent.
   - d is known as the secret exponent or decryption exponent.

### 4.3. CONSENSUS Algorithms:

- **PoW:** (Proof of work) could be an accord strategy employed in the Bitcoin network. In PoW, every node of the network is shrewd a hash worth of the block header. The block header contains a nowadays and miners would modification the nowadays often to induce completely different hash values. The accord needs that the calculated worth should be adequate to or smaller than a specifically given worth. PoS: (Proof of stake) is a vitality sparing option in contrast to PoW. Diggers in PoS need to demonstrate the responsibility for the measure of money. Specifically, Blockchain utilizes randomization to anticipate the next generator. It utilizes an equation that searches for the most minimal hash an incentive in blend with the span of the stake. Numerous blockchains embrace PoW toward the start and change to PoS bit by bit.
- **PBFT:** (Practical byzantine fault tolerance) is a replication calculation to endure byzantine issues. Hyperledger Fabric uses the PBFT as its 34-accord calculation since PBFT could deal with up to 1/3 malignant byzantine reproductions. DPOS: (Delegated proof of stake) is agent fair. Partners choose their agents to produce and approve squares. Cast a ballot out effectively. DPOS is the foundation of Bitshares. Ripple: Ripple is an accord calculation that uses, by and large, confided in subnetworks inside the bigger System. In the System, hubs are separated into two kinds: server for taking an interest accord process and customer for just exchanging assets.
- **Consensus Protocol Rules:** Consensus rules are a certain set of rules that works on the network will confirm that a block follows only after validating the same along with the transactions. The primary requirement to achieve a consensus is a unanimous acceptance between nodes on the network for a single data value, even in the event of some of the nodes failing or being unreliable in any way.

### 4.4. Tools:

- **MS Visual Studios:** Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop computer programs, as well as websites, web apps, web services and mobile apps. Visual Studio uses Microsoft software development platforms such as Windows API, Windows Forms, Windows Presentation Foundation, Windows Store and Microsoft Silverlight. It can produce both native codes and managed code. Visual Studio includes a code editor supporting IntelliSense (the code completion component) as well as code refactoring. The integrated debugger works both

ISSN PRINT 2319 1775 Online 2320 7876
Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 5, 2022

as a source-level debugger and a machine-level debugger. Other built-in tools include a code profiler, forms designer for building GUI applications, web designer, class designer, and database schema designer.

- **Android Studio:** Android Studio is the official integrated development environment (IDE) for Google's Android operating system, built on JetBrains' IntelliJ IDEA software and designed specifically for Android development. It is available for download on Windows, macOS and Linux based operating systems.[9][10] It is a replacement for the Eclipse Android Development Tools (ADT) as the primary IDE for native Android application development.

## III. SULTS

Input: Request of the user (send data to the cloud or retrieve data from the cloud).
Output: Requested data of the user.
Following outcomes were observed: -

1. er can access the data and the ERP system.
2. min can authenticate the user request.
3. min can set permission to users.
4. min can monitor all data transaction done by all users.
5. er can authenticate his access using 2-step authentications (Biometrics).

## IV. LUSION

The implemented a new blockchain-based solution for data usage auditing relying on the use of hierarchical ID-based mechanisms. Acting as a delegated PKG, each data owner can provide consent on his data usage and to control data collection and processing activities, in a privacy-preserving manner based on smart contract approach. In addition, our solution enables service providers to have proof of receiving the data owners consent before processing his personal data, as the blockchain architecture is computationally tamper-proof. Big Data Industry: System can be used in big data industries as a service purpose, i.e. companies can provide this service to their client. Institutes: Vital information of institute like employee data, project report can be stored on the cloud using this System. Web applications: In web applications where only a specific amount of data is to be displayed out of entire data, this application can be used.

## V. E SCOPE

The system currently works on only a prescribed combination system OS; it can be designed to work on any combination of OS. Currently, the System handles only one type of data; it can be designed to work with any type of data. The system can be made more affordable, depending on the use of the user.

## VI. EDGEMENT

We are very thankful to our guide Prof. C. R. Patil, K. K. Wagh Institute of Engineering Education & Research, Nashik for the guidance we needed and her indispensable support, suggestions.

## VII. REFERENCES

**[1]** X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability, in: International Symposium on Cluster, Cloud and Grid Computing, IEEE/ACM, 2017.

**[2]** D. Tosh, S. Sengupta, C. A. Kamhoua, K. A. Kwiat, Establishing evolutionary game models for cyber security information exchange (cybex), Elsevier Journal of Computer and System Sciences. URL http://dx.doi.org/10.1016/j.jcss.2016.08.005.

**[3]** D. K. Tosh, M. Molloy, S. Sengupta, C. A. Kamhoua, K. A. Kwiat, Cyberinvestment and cyber-information exchange decision modeling, in: IEEE 7th International Symposium on Cyberspace Safety and Security,2015, pp.12191224.

**[4]** E. Heilman, A. Kendler, A. Zohar, S. Goldberg, Eclipse attacks on bitcoins peer-to-peer network, in: 24th USENIX Security Symposium (USENIX Security 15), 2015, pp. 129144.

**[5]** A. Biryukov, D. Khovratovich, I. Pustogarov, Deanonymisation of clients in bitcoin p2p network, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2014, pp. 1529.

**[6]** X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability, in: International Symposium on Cluster, Cloud and Grid Computing, IEEE/ACM, 2017.

**[7]** C. Europe. Proposal for a regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. In General Data Protection Regulation, January 2016, 2016.

**[8]** M. Swan. Blockchain: Blueprint for a new economy. OReilly Media, Inc., 2015.

ISSN PRINT 2319 1775 Online 2320 7876
*Research paper*  **UGC CARE Listed ( Group -I) Journal Volume 11, Iss 5, 2022**

**[9]** G. Zyskind, O. Nathan, and A. Pantland. Decentralizing privacy: Using blockchain to protect personal data. In IEEE Security and Privacy Workshops (SPW), 2015.

**[10]** GSA, Cloud Computing Initiative Vision and Strategy Document (DRAFT), http://info.apps.gov/sites/default/files/ Cloud-Computing-Strategy-0.ppt.

**[11]** S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

**[12]** State of blockchain q1 2016: Blockchain funding overtakes bitcoin, 2016. [Online]. Available: http://www.coindesk.com/ state-of-blockchain-q1-2016/

**[13]** Ibrar Ahmed, Shilpi, Mohammad Amjad, Blockchain Technology A Literature Survey, International Research Journal of Engineering and Technology (IRJET), 2018.