Blockchain based Security in Cloud Computing

A.P.Gopu, Prawin N, Thirugnanasambantham N, Sukant B

Assistant Professor,
Department of Computer Science Engineering,
Velalar College of Engineering and Technology, Erode, TamilNadu
Student,Department of Computer Science Engineering, VelalarCollegeofEngineeringand Technology,
Erode,TamilNadu.

Abstract-Maintaining data security and integrity is very important in cloud computing since data can be tampered with and malicious attackers could use this to their advantage. Most Cloud service providers only focuses on providing security in cloud servers and relies on third parties for ensuring data integrity. Our project is aimed to ensure the integrity of data in cloud servers by using block chain which is known to be highly secure. Network storage services have benefited countless users worldwide due to the notable features of convenience, economy and high availability. Since a single service provider is not always reliable enough, more complex multi-cloud storage systems are developed for mitigating the data corruption risk. While a data auditing scheme is still needed in multi-cloud storage to help users confirm the integrity of their outsourced data. Unfortunately, most of the corresponding schemes rely on trusted institutions such as the centralized third-party auditor (TPA) and the cloud service organizer, and it is difficult to identify malicious service providers after service disputes. Therefore, we present a block chain-based multi-cloud storage data auditing scheme to protect data integrity and accurately arbitrate service disputes. The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data Retrieval from the cloud.

I.INTRODUCTION

Cloud advances are becoming effective arrangements that permit hubs to speak with one another in these limit organizing conditions. Regularly, when there is no limit to end association between a source and an objective pair, the messages from the source hub might have to sit tight in the halfway hubs for a significant measure of time until the association would be in the end laid out. Remote Sensor Network (WSN) advances are becoming effective arrangements that permit hubs to speak with one another in these limit organizing conditions. Regularly, when there is no limit to end association between a source and an objective pair, the messages from the source hub might have to sit tight in the middle hubs for a significant measure of time until the association would be in the end laid out.

In Military organization situations, associations of remote gadgets conveyed by fighters might be briefly separated by sticking, ecological variables, and portability, particularly when they work in unfriendly conditions. Roy and Chuah presented capacity hubs in WSNs where information is put away or recreated with the end goal that main approved versatile hubs can get to the fundamental data rapidly and effectively. Numerous tactical applications require expanded security of classified information including access control strategies that are cryptographically implemented. Much of the time, it is attractive to give separated admittance administrations with the end goal that information access strategies are characterized over client ascribes or jobs, which are overseen by the key specialists. For instance, in a disturbance lenient military organization, a commandant might store a private data at a capacity hub, which ought to be gotten to by individuals from "Brigade 1" who are partaking in "Locale 2." For this situation, it is a sensible presumption that various key specialists are probably going to deal with their own powerful characteristics for fighters in their sent districts or echelons, which could be habitually different (e.g., the quality addressing current area of moving troopers). It alludes to this WSN engineering where numerous specialists issue and deal with their own property keys freely as a decentralized WSN.

The idea of characteristic based encryption (ABE) is a promising methodology that satisfies the prerequisites for se-fix information recovery in WSNs. ABE highlights a system that empowers an entrance command over encoded information utilizing access strategies and credited credits among private keys and cipher texts. Particularly, cipher text-strategy ABE (CP-ABE) gives a versatile approach to encoding information to such an extent that the encrypt tor characterizes the characteristic put that the decrypt or needs to have together to de-grave the cipher text. In this manner, various clients are permitted to unscramble various bits of information per the security strategy. In any case, the issue of applying the ABE to WSNs presents a few security and protection challenges. Since certain clients might change their related traits eventually (for ex-more than adequate, moving their area), or some confidential keys may be compromised, key repudiation (or update) for each property is fundamental to make frameworks secure. Notwithstanding, this issue is considerably more troublesome, particularly in ABE frameworks, since each at-recognition is possibly shared by various clients (hence, it allude to such an assortment of clients as a quality gathering). This suggests that repudiation of any characteristic or any single client in a property gathering would influence different clients in the gathering. For ex-adequate, in the event that a client joins or leaves a quality gathering, the related characteristic key ought to be changed and rearranged to the wide range of various individuals in a similar gathering for in reverse or forward mystery. It might bring about bottleneck during rekeying technique, or security debasement because of the windows of weakness in the event that the past trait key isn't refreshed right away.

Another test is the key escrow issue. In CP-ABE, the key authority produces private keys of clients by applying the power's lord secret keys to clients' related arrangement of at-accolades. Subsequently, the key authority can unscramble each cipher text addressed to explicit clients by creating their trait keys. In the event that the key authority is undermined by enemies when conveyed in the unfriendly conditions, this could be an expected danger to the information classification or security particularly when the information is profoundly delicate. The key escrow is an inborn issue even in the different power frameworks insofar as each key authority has the entire honor to produce their own characteristic keys with their own lord mysteries. Since such a key age component in light of the single expert mystery is the fundamental strategy for the greater part of the deviated encryption frameworks, for example, the at-recognition based or personality based encryption conventions, eliminating escrow in single or various power CP-ABE is a vital open issue. The last test is the coordination of characteristics gave from various specialists. At the point when various specialists oversee and give characteristic keys to clients freely with their own lord insider facts, it is exceptionally difficult to characterize fine-grained admittance arrangements over credits gave from various specialists.

II. LITERATURE REVIEW

This paper [1] proposed a Multi-Authority Trait Based Encryption (ABE) framework. In our framework, any party can turn into a power and there is no prerequisite for any worldwide coordination other than the production of an underlying arrangement of normal reference boundaries. A party can essentially go about as an ABE authority by making a public key and giving confidential keys to various clients that mirror their characteristics. A client can encode information as far as any Boolean recipe over credits gave from any picked set of specialists. At last, this framework requires no focal power. In building this framework, our biggest specialized obstacle is to make it arrangement safe. Earlier Property Based Encryption frameworks accomplished plot obstruction when the ABE framework authority tied" together various parts (addressing various qualities) of a client's confidential key by randomizing the key.

This paper [2] presents a new methodology for realizing Cipher text-Policy Attribute Encryption (CPABE) under concrete and non-interactive cryptographic assumptions in the standard model. This solutions allow any en crypto to specify access control in terms of any access formula over the attributes in the system. In our most efficient system, cipher text size, encryption, and decryption time scales linearly with the complexity of the access formula. The only previous work to achieve these parameters was limited to a proof in the generic group model. It presents three constructions within our framework. This first system is proven selectively secure under a assumption that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption. This next two constructions provide performance trades to achieve provable security respectively under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions.

This paper [3] focused on an important issue of attribute revocation which is cumbersome for CP-ABE schemes. In particular, it resolve this challenging issue by considering more practical scenarios in which semi trustable on-line proxy servers are available. As compared to existing schemes, this proposed solution enables the authority to revoke user attributes with minimal effort. It achieved this by uniquely integrating the technique of proxy re-encryption with CP-ABE, and enabled the authority to delegate most of laborious tasks to proxy servers. This proposed scheme is provably secure against chosen cipher text attacks. In addition, it shows that this technique can also be applicable to the Key-Policy Attribute Based Encryption (KP-ABE) counterpart.

This paper [4] proposed a new way to mitigate the limitation of IBE with regard to revocation, and improve efficiency of the previous solution. It want to remove interaction form the process of key update, as keeping the PKG online can be a bottleneck, especially if the number of users is very large. At the same time we do not want to employ trusted hardware and we want to significantly minimize the work done by the PKG and users. First we define the Revocable IBE primitive and its security model that formalizes the possible threats. The model, of course, takes into account all adversarial capabilities of the standard IBE security notion. I.e. the adversary should be able to learn the private keys of the users with identities of its choice, and in the case of chosen-cipher text attack to also see decryptions under the private key of the challenge identity of the cipher texts of its choice. The adversary should not be able to learn any partial information about the messages encrypted for the challenge identity.

This paper [5] apply the Canetti-Halevi-Katz procedure to get a picked cipher text (CCA) secure expansion utilizing one-timing schemes. The security verification is a decrease to the DBDH suspicion and the solid existential unforged ability of the mark crude. What's more, we acquaint various leveled ascribes with improve our essential plan — diminishing both cipher text size and encryption/unscrambling time while keeping up with CPA security. At last, it propose an expansion where access strategies are inconsistent edge trees, and it finish up with a conversation of viable utilizations of CP-ABE.

III. EXISTING SYSTEM

Network capacity administrations have helped incalculable clients overall because of the prominent elements of comfort, economy and high accessibility. Since a solitary specialist co-op isn't generally sufficiently dependable, more intricate multi-distributed storage frameworks are produced for moderating the information debasement risk. While an information evaluating plan is as yet required in multi-distributed storage to assist clients with affirming the respectability of their re-appropriated information. Tragically, the majority of the comparing plans depend on confided in foundations like the concentrated outsider examiner (TPA) and the cloud administration coordinator, and it is hard to recognize noxious specialist organizations after help disputes. Therefore, we present a block chain based multi-distributed storage information reviewing plan to safeguard information trustworthiness and precisely arbitrate administration questions. The idea of property based encryption (ABE) is a promising methodology that satisfies the prerequisites for secure information recovery in WSNs. ABE highlights a component that empowers an entrance command over encoded information utilizing access strategies and credited ascribes among private keys and cipher texts. Especially, cipher text-strategy ABE (CP-ABE) gives a versatile approach to scrambling information to such an extent that the encrypt or characterizes the property put that the decrypt or needs to have together to de-grave the cipher text. Thus, various clients are permitted to unscramble various bits of information per the security policy. ABE comes in two flavor’s called key-strategy ABE (KP-ABE) and cipher text-strategy ABE (CPABE). In KP-ABE, the encrypt or just will mark a cipher text with a bunch of attributes. The key authority picks a strategy for every client that figures out which cipher texts he can decode and gives the way in to every client by implanting the approach into the client's vital. In any case, the jobs of the cipher texts and keys are turned around in CP-ABE.

The majority of the current ABE plans are built on the design where a solitary believed authority has the ability to produce the entire confidential keys of clients with its lord secret information. Thus, the key escrow issue is inborn to such an extent that the key authority can unscramble each cipher text addressed to clients in the framework by creating their mystery keys at any time. Bettencourt et al. furthermore, Boldyrev a et al. first proposed key repudiation components in CP-ABE and KP-ABE, separately. Their answers are to add to each credit a lapse date (or time) and disperse another arrangement of keys to legitimate clients after the termination. The intermittent trait revocable ABE plans have two principal issues. The first issue is the security corruption in quite a while of the regressive and forward secrecy. It is a significant situation that clients, for example, fighters might change their traits regularly, e.g., position or area move while considering these as characteristics. Then, at that point, a client who recently holds the quality could possibly get to the past information encoded before he gets the property until the information is re encrypted with the newly updated trait keys by intermittent rekeying (in reverse secrecy).Chase et al. introduced a circulated KP-ABE plot that takes care of the key escrow issue in a multi authority framework. This methodology, all (disjoint) property specialists are partaking in the key age convention in a dispersed way to such an extent that they can't pool their information and connection different trait sets having a place with a similar user. One detriment of this completely disseminated approach is the exhibition debasement. Since there is no unified authority with ace restricted data, all quality specialists ought to speak with one another in the framework to create a client's mystery key. This outcomes in correspondence above on the framework arrangement and the rekeying stages and requires every client to store extra assistant key parts other than the qualities keys, where is the quantity of experts in the system. Huang et al. furthermore, Roy et al. proposed decentralized CP-ABE plans in the multi authority network climate. They accomplished a consolidated admittance strategy over the properties gave from various specialists by essentially scrambling information numerous times. The principal inconveniences of this approach are effectiveness and expressiveness of access policy. For model, when a leader encodes a mysterious mission to fighters under the arrangement ("Legion 1" AND ("District 2" OR 'Locale 3")), it can't be communicated when every "District" property is overseen by various specialists, since basically multi scrambling approaches can in no way, shape or form express any broad " - out-of-" rationales (e.g., OR, that is 1-out-of-).

A. *DRAWBACK OF EXIXTING SYSTEM*

- Most of the corresponding schemes rely on trusted institutions such as the centralized third-party auditor (TPA) and the cloud service organizer, and it is difficult to identify malicious service providers after service disputes.
- Immutability can only exist if network nodes are fairly distributed.
- The problem of applying the ABE to WSNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for ex-ample, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure.

IV. PROPOSED SYSTEM

We propose a protected multi-proprietor information sharing plan. It suggests that any client in the gathering can safely impart information to others by the UN trusted cloud. Our proposed plot can uphold dynamic gatherings proficiently. In particular, new allowed clients can straightforwardly decode information records transferred before their cooperation without reaching with information proprietors. Client renouncement can be effortlessly accomplished through original repudiation list without refreshing the mystery keys of the excess clients. The size and calculation above of encryption are consistent and free with the quantity of denied clients. We give secure and protection safeguarding access control to clients, which ensures any part in gathering to use the cloud asset secretly. Additionally, the genuine characters of information proprietors can be uncovered by the gathering director when questions happen. SHA-256 (Secure Hash Calculation) is utilized as the proposed model

Propose a protected information recovery conspire involving CP-ABE for decentralized WSNs where numerous key specialists deal with their traits independently. It shows how to apply the proposed component to safely and proficiently deal with the classified information conveyed in the disturbance open minded military network. First, prompt quality disavowal improves in reverse/forward mystery of secret information by decreasing the windows of vulnerability. Second, encrypt or can characterize a fine-grained admittance strategy utilizing any droning access structure under credits gave from any picked set of authorities. Third, the key escrow issue is re-tackled by a without escrow key giving convention that takes advantage of the trait of the decentralized WSN engineering.

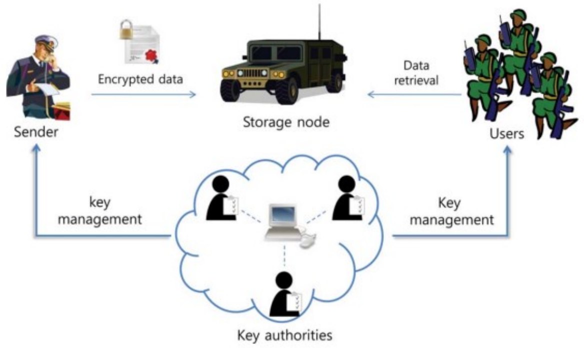
The key giving convention creates and gives client secret keys by per-shaping a safe two-party calculation (2PC) convention among the vital specialists with their own lord insider facts.

The 2PC convention dissuades the critical specialists from getting any expert privileged intel of one another to such an extent that not a single one of them could produce the entire arrangement of client keys alone. In this way, clients are not expected to completely trust the experts to safeguard their information to be shared.

The information secrecy and security can be crypto-graphically authorized against any inquisitive key specialists or information stockpiling hubs in the proposed plot.

A. ADVANTAGES OF PROPOSED SYSTEM

- Provides a flexible stack of massive computing, storage, and software services in a scalable manner.
- Support on fast detection and locating of errors in big sensor data sets.
- To efficiently utilize the computation power and massive storage, the detection and location tasks can be distributed to cloud platform.
- No Third Party Administrator is needed.
- Block chain based self-key authority.



B. SYSTEM ARCHITECTURE

V. MODULE DESCRIPTION

A. KEY GENERATION

Key Specialists are key age places that produce public/secret boundaries for CPABE. The key specialists comprise of a focal power and numerous neighborhood specialists. It expects that there are secure and dependable correspondence channels between a focal power and every nearby authority during the underlying key arrangement and age stage. Every neighborhood authority oversees various characteristics and issues comparing quality keys to users. They award differential access freedoms to individual clients in view of the clients' credits. The key specialists are thought frankly yet inquisitive. That is, they will genuinely execute the relegated errands in the framework, but they might want to learn data of scrambled contents however much as could reasonably be expected.

B. MULTIAUTHORITY CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION

Source is a substance who possesses classified messages or information (e.g., a leader) and wishes to store them into the outer information stockpiling hub for simplicity of sharing or for solid conveyance to clients in the limit organizing environments. A shipper is answerable for central (trait based) access strategy and upholding it on its own information by scrambling the information under the strategy prior to putting away it to the capacity node. After the development of cipher text, the source stores it to the capacity hub safely. On getting any information demand inquiry from a client, the capacity hub answers with to the user. The shipper can characterize the entrance strategy under traits of any picked set of various specialists with practically no limitations on the rationale expressiveness rather than the past multi authority plans.

C. STORE IN STORAGE NODE

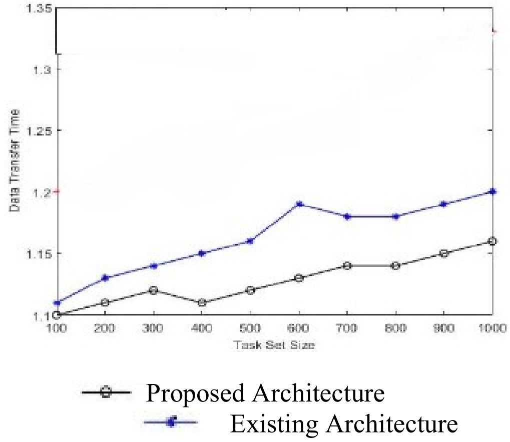
Capacity hub is a substance that stores information from shippers and give relating admittance to users. It might be versatile or static. Like the past plans, it additionally expects the capacity hub to be semi trusted, that tells the truth however curious. The client needs to get to the information put away at the capacity hub, it gives the comparing cipher text.

D. MULTIAUTHORITY CIPHERTEXT-POLICY ATTRIBUTE-BASED DECRYPTION

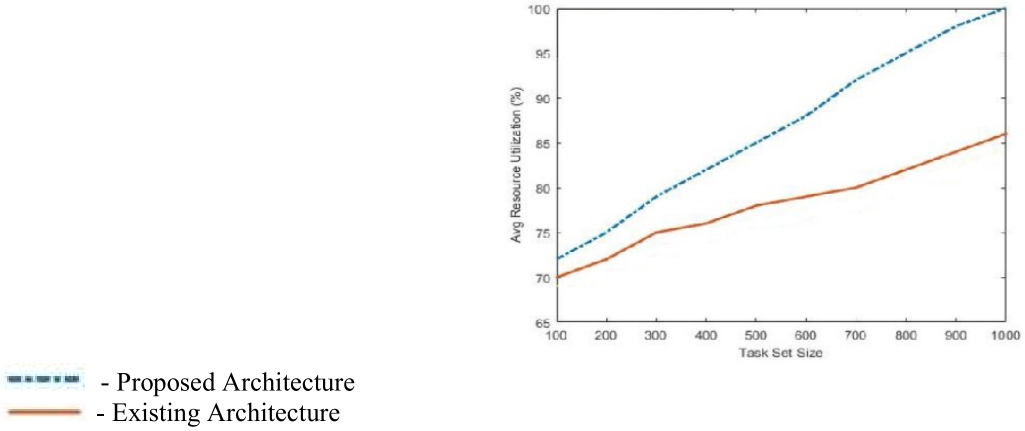
Client is a versatile hub who needs to get to the information put away at the capacity hub (e.g., a warrior). On the off chance that a client has a bunch of characteristics fulfilling the entrance strategy of the encoded information characterized by the source, and isn't disavowed in any of the qualities, then, at that point, he gets the cipher text from the capacity hub, the client unscrambles the cipher text with its mystery key utilizing Multi authority Cipher text-Strategy Trait Based Decryption. Then get the information.

VI.EXPERIMENT AND RESULT

One of the basic components of calculating execution time is the data files transfer time incurred by transferring data files from the remotely located storage resources to the decoupled computing resources if the required files are not locally available. In our experiments, the percent share of the data files transfer time in the makes pan calculation is evaluated. The following Figure plot the impact of the average data transfer time for the task sets.



GRAPH COMPARISON BETWEEN EFFECT OF DATA TRANSFER TIME ON TASK SETS



GRAPH COMPARES THE EFFECT ON RESOURCE UTILIZATION ON DIFFERENT ARCHITECTURES

As seen in the above figure the proposed architecture is reactive in the context of efficient utilization of cloud resources than the existing architecture.

VI. CONCLUSION

To reduce the computational power and increase the speed in accessing the files from the cloud , we propose a secure transmission architecture using the cipher text policy based encryption. We conducted simulations and implemented prototypes of the architecture. Both simulation and experimental results show that can achieve higher effective secret transmission rate than that of existing architecture, which verify the theoretical analysis.

REFERENCES

[1] Lewko and B. Waters, "Decentralizing trait based encryption," Cryptology ePrint Chronicle: Rep. 2020/351, 2020.

[2] C.Nagarajan and M.Madheswaran - ‘Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter’ - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[3] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. “Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter” Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-strategy trait based encryption," in Proc. IEEE Symp. Security Protection, 2019, pp. 321-334

[5] C.Nagarajan and M.Madheswaran - ‘Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis’- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[6] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash “Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM”SurajPunj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756

[7] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, “Perfromance Investigation of T-Source Inverter fed with Solar Cell” SurajPunj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749

[8] C.Nagarajan and M.Madheswaran - ‘Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques’- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[9] Boldyreva, V. Goyal, and V. Kumar, "Personality based encryption with proficient repudiation," in Proc. ACM Conf. PC. Local area. Security, 2019, pp. 417-426.

[10] L. Cheung and C. Newport, "Provably secure ciphertext strategy ABE," in Proc. ACM Conf. Comput. Commun. Security, 2020 pp. 456-465.

[11] Nagarajan and M.Madheswaran - ‘Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis’- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September2012.

[12] G.Neelakrishnan, R.S.Jeevitha, P.Srinisha, S.Kowsalya, S.Dhivya, “Smart Gas Level Monitoring, Booking and Gas Leakage Detector over IOT” International Journal of Innovative Research in Science, Engineering and Technology, March 2020, Volume 9, Issue 3, pp: 825-836

[13] M. Chase and S. S. M. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” in Proc. ACM Conf. Comput. Commun. Security, 2019, pp. 121–130.

[14] M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Hysyanskaya, and H. Shacham, “Randomizable proofs and delegatable anonymous credentials,” in Proc. Crypto, LNCS 5677, pp. 108–125 M.