International Journal of Computer Science & Communication (ISSN: 0973-7391)
Special Issue, Page71-75, December 2020 ------ available at www.csjournals.com

Cloud System Implementation using Block Chain with Authentication Security and Systematic Approach

Shobha Rani N R[1]
PG Student
Dept. of CS&E, SSIT, Tumkur

Dr. Channakrishna Raju[2]
Associate Professor
Dept. of CS& E, SSIT, Tumkur

Dr. M Siddappa[3]
Head of Dept.
Dept. of CS&E, SSIT, Tumkur

***Abstract*—** In a Cloud processing environment, when information or data is put on a Cloud, individual-related information might be leakage through the exhibition. To maintain a strategic distance from this we are utilizing zero information confirmation to the shrewd framework and a strategy for demonstrating a work without uncovering the data outside. Data like public key and we have doing investigate on the best way to improve the centrality for security insurance. In association here chipping away at the proposition clarifies the productive booking of workers with multi rest mode for the cloud server farm.

Starting late, the imperativeness usage of cloud worker ranches has continued growing. Incalculable workers run at a low use rate, which achieves an unprecedented abuse of force. To save greater imperativeness in a cloud worker ranch, we propose an essentialness beneficial task booking instrument with turning on/rest technique for workers in the virtualized cloud worker ranch. Key idea is that when the amount of latent VMs shows up at a foreordained edge, the worker with the idlest VMs will be changed to rest mode in the wake of moving all the running tasks to various workers. From the perspective of the hard and fast number of tasks and the amount of workers in rest mode in the system, we set up a Zero-Knowledge confirmation, a block chain secrecy improvement innovation, was acquainted with forestall security dangers, for example, individual data encroachment through block request

Index Terms: Cloud; Public Key; Privacy Protection

I. INTRODUCTION

The IoT is the shortening of the Internet of Things, which empowers objects to share and control information between objects since things are associated with the Internet. It is conceivable to submit malevolent assaults, for example, information altering, or security encroachment, while sharing information on items over the Internet. This paper acquainted a block chain with forestall security dangers, for example, information forging, which could happen utilizing brilliant meters. Zero-Knowledge verification, a block chain obscurity upgrade innovation, was acquainted with forestall security dangers, for example, individual data encroachment through block request. It was proposed to utilize brilliant agreements to forestall savvy meter information phony and individual data encroachment we recommend. One of the critical clarifications behind essentialness inefficiency is the abuse of inactive power when worker ranch workers are giving preparing and limit

capacities at low utilization rates Hindawi Mathematical Problems in Engineering [7]. i.e., task booking computations fundamentally influence the imperativeness use of colossal worker ranches [3]. , thusly, how to improve worker use to save essentialness has become an inconvenient issue in cloud worker cultivates that basically should be settled. Also, the brisk improvement of predominant figuring methodologies requires extended response execution in cloud worker, tradeoff between essentialness use and response execution has moreover become a hot examination subject [1].

II.RELEATED WORK

Smart networks are astute lattices that consolidate IT innovation with customary matrices to upgrade the effectiveness of the energy usage [1]. In a smart matrix climate, each Advanced Mitigation Infrastructure (AMI) is sent in clients and can be utilized to quantify energy creation and use and offer types of assistance, for example, resale [2]. In a shrewd lattice climate, brilliant meters are expected to gauge power utilization. The savvy meter is introduced toward the finish of every gadget to record the force utilization and creation of the gadget, and the collected information can examine the force use design [3]. Security weaknesses for keen meters have protection worries that examine designs utilizing power use snoopping and traffic investigation [4]. There is additionally the danger of directing the force information communicated sent from the keen meter to charge lower or greater expenses. So we have to present brilliant meter confirmation innovation [5].

Block chain has been applied to bit coin and ethereum utilizing security innovations, for example, electronic marks, public keys, and hash capacities. The spot coin created by Satoshi Nakamoto is getting consideration, and it is additionally contemplating the use strategy in monetary and non-monetary regions including virtual money. In the touch coin, the block chain is a sort of disseminated computerized book that stores the historical backdrop of the spot coin, which is a cash, given occasionally [7]. This record is made of cryptographic strategies that can't be falsified or tweaked and is made as a confirmation step to forestall imitation and altering of exchanges through exchange cycles and hash esteems as appeared in Figure 1 for the exchange of ownership[8].

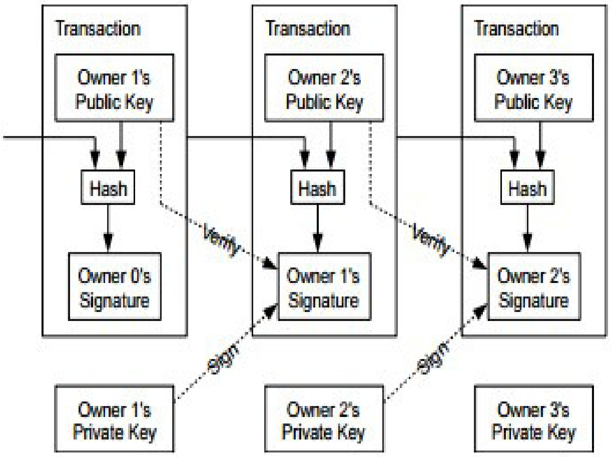


Fig. 1. Transactions in a block chain

A Zero knowledge proof is a method of proving that information is known without disclosing any information. The concept of the zero knowledge proof introduced in the block chain is a proof method that can prove a transaction or a work without exposing the information or transaction information of the virtual money to the outside. It is a proof method which satisfies three properties of completeness, impracticality, and Zero Knowledge.

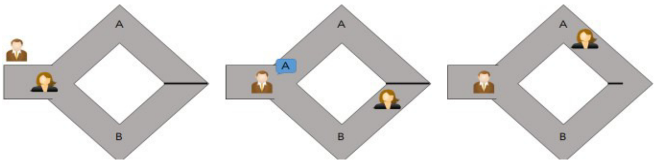


Fig. 2. Examples of Zero Knowledge Proof

In Figure 2, the content of the paper that introduces the zero knowledge proof to the cave easily is illustrated [14]. The prover can open the door through the secret key, and the verifier does not know the secret key, but verifies that the prover is correct. The prover enter to the secret door with road of A or B , and the verifier tells the prover to return to road of A. If the prover knows the secret key, the probability of the prover coming back is 100%. However, even if you do not know the secret key that is not a prover, the likelihood of returning via A is 50%. If you continue these process n times, the probability of not returning will increase if you are not a prover. This method of verification through probability is called the proof of zero knowledge. In other words, by using the zero knowledge proof in the block chain, the verifier can confirm that the transaction party is correct without knowing the information of the transaction party, transaction contents.

III. PROPOSAL OF AUTHENTICATION AND DATAPROTECTION SYSTEM USING BLOCK CHAIN

As a proposed framework environment, contains the client is putting away information in cloud by utilizing task scheduler. In the below system, the structure ponders the issue of restricting imperativeness usage of a data center by booking workers in multi rest modes moreover, at different repeat levels to diminish the total essentialness of dynamic workers. That is, given the presence of customer requests, plan the workers (to dynamic state with different frequencies or to different rest states), with the ultimate objective that the hard and fast imperativeness use of the worker ranch can be restricted while satisfying the QoS essential. The booking count will choose: 1) what number of the dynamic workers should be traded into which rest state in each timeslot; 2) what number of the napping workers in rest states should be woken up in each timeslot; 3) what repeat levels should the dynamic workers be set to in each timeslot.

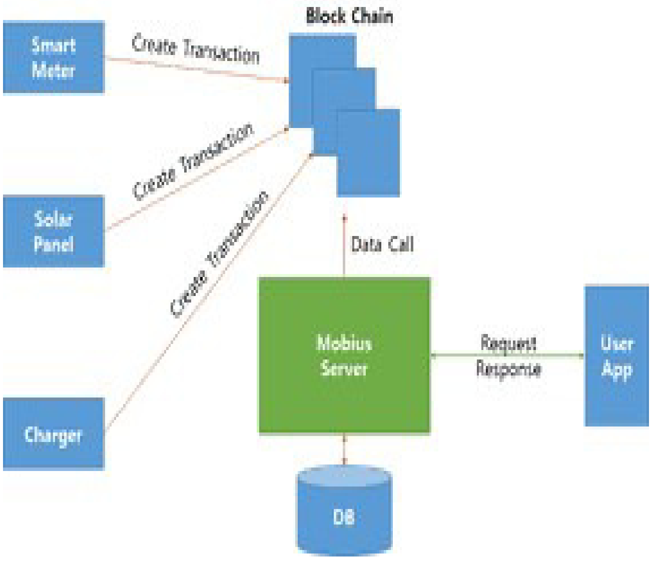


Fig 3. Proposed system architecture

Figure 3 shows the proposed system architecture configuration of smart grid system including task queue, VM manager and virtual machines. Each device has a module for measuring the amount of power and stored in a block-chain smart contract function depending on the situation. In general electric users, the electricity used through the smart meter is stored together with the usage time, and in the case of the prosumer, the electric prduction is stored in the smart contract. In the case of an electric car charger, when a consumer plugs in a charger, the electricity generated by the prosumer is consumed, the electricity consumed is stored in the contract, and the electricity generated by the prosumer is reduced and stored. Through the application, the general user can search the used electricity quantity and pay the electricity bill according to the period with call the smart contract function.

The prosumer can search for the electricity generated and the consumer using the electric car charger can search the charger to find the amount of electricity that can be charged and the amount of electricity charged by the vehicle.

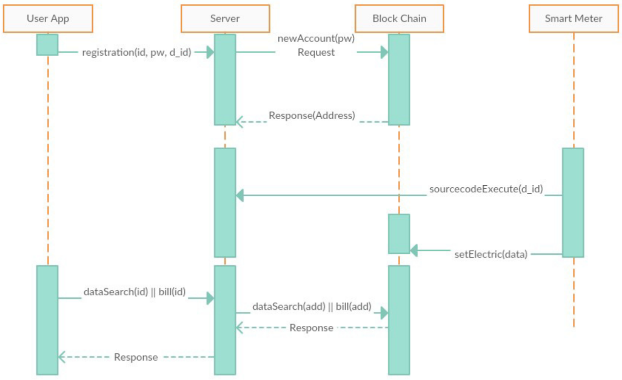


Fig 4. Device authentication and data transmission sequence diagram

In the proposed system, the authentication method and the data transmission method of the smart meter are the same as the sequence diagram of Figure 5. The user transmits the 'device ID' and 'user ID' and 'password to be used as the block chain password' of the smart meter through the Mobius server to register the member. The Mobius server requests a new account in the block chain with the password from the transmitted member information and receives the account address response. Mobius stores the user ID, device ID, and account address sent to the member application in the database. When the Smart Meter is executed, the Smart Meter receives and executes the power measurement source code stored in the server by ftp, and stores the amount of power consumed by the Smart Contract in the block chain by selecting the account address in the server's database. The smart contract accumulates the power data transmitted from the smart meter and requests the transaction by calculating the charge by the calculation method applying the progressive tax on the day and month. After the block is created, the user sends the member ID to the Mobius server to retrieve the power consumption or to pay the fee, and the server retrieves the data uploaded to the block through the block chain address matched to the ID in the database and displays it in the user application.

In the proposed system, if the verifier or a third party knows only the address of the user, the amount of power consumed and the amount of the fee paid can be inquired through the lock. This is a problem of personal information infringement because it can analyze the power consumption pattern of the user. An attacker is at risk of a second crime, such as theft, because the user can see if the house is empty. Therefore, in this paper, we propose a method to protect the personal information of the proposed system by adding a proof of zero knowledge that can prove the information is correct without providing information to the verifier.

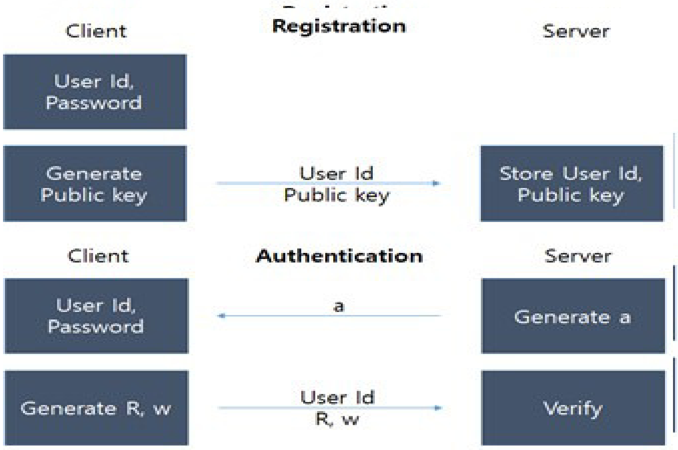


Fig 5. Zero Knowledge Proof Authentication Protocol

As shown in Figure 6, the client generates a public key and stores it together with the ID, unlike the system that hashes the existing password to the server directly. This has the advantage of preventing cracking breaking the hash encryption of existing systems. It is a protocol that can be proved without sending a hashed password to the server when the user login[16].

Using the zero knowledge proof authentication protocol, the public key is stored in the block chain without storing the original data in the block chain, and the original data is stored in the server database. When the proof is completed through the zero knowledge proof process together with the public key stored in the block chain, the data is called so that the data can be prevented from being modulated. It also protects your privacy because you do not put your original data directly in the block chain.

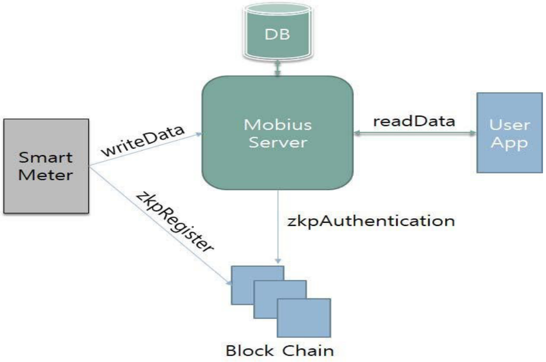


Fig 6. Zero knowledge proof block chain system diagram

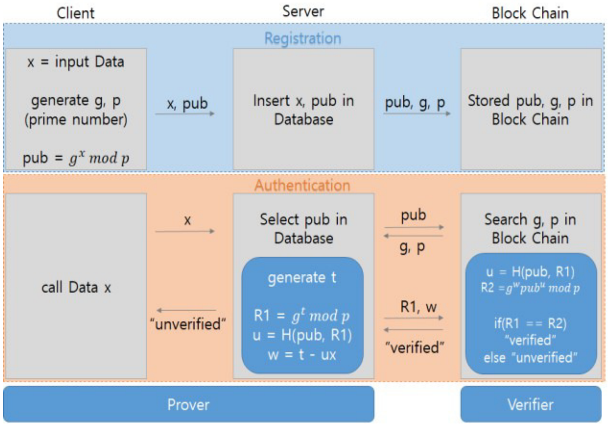


Fig 7. Block Chain Authentication and Data Protection Proposal System using Zero Knowledge

As shown in Figure 7, the proposed system consists of registration and authentication a two-step process and a three stages of client, server, and block chain. In the block chain, the registration phase and the authentication phase are implemented as a non - interactive zero knowledge verification[19] function using the smart contract. In the registration step, the data x to be protected by the client is input to generate a random number g and p, which are prime numbers, and the data is regarded as a secret key, and a public key pub is generated. The data x to be protected on the server and the generated pub are transmitted and the server stores it in the database. Also, in the block chain, the random values g and p and the public key pub generated without transmitting the data x to be protected are transmitted and stored in the block to complete the registration. When calling the data in the proposed system, the authentication process is performed. When the client calls the data x stored in the server, it selects the public key pub of x stored in the server's database. In the stored block chain, if the query is made through pub, the random values g and p stored in the registration step are called. Through the g and p transmitted from the block chain, the server generates R1 and w by the non-interactive zero knowledge proof with low communication burden, and transmits to the block chain. The smart contract in the block chain executes the proof function using the received R1 and w and computes the value of R2. Through this, it can be proved that the value of stored data x in the server cannot be modulated even if it is not stored directly in the block chain.

IV. SECURITY ANALYSIS

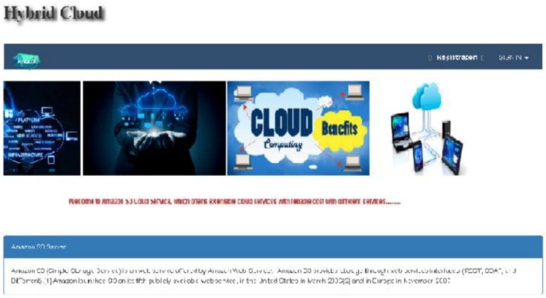
Data collected through smart meters is used for power pricing. Therefore, the collected data must be integrity protected to prevent it from being tampered with. For example, a user might want to pay less than the amount of power user used, so user is likely to tamper with the data. In addition, the power provider is likely to modulate the data to charge more power charges than the user has consumed.

Therefore, it is possible to generate blocks by verifying the data transmitted by the smart meter and to disperse the ledger to make data impossible to be modulated and to maintain integrity.

Also, if the data collected through the smart meter is cattered and distributed among several people by the block chain, the malicious attacker can analyze the life pattern of the user by searching the power consumption over time, and the attacker can save the time consuming the minimum power consumption Based on this, the attacker can know whether user is going out or vacationing. As such, if the data collected through the smart meter is directly exposed by the block chain, it may infringe the privacy of the user and damage the property of the user. In the proposed system, the public key generated by proving zero knowledge is stored in order to maintain confidentiality without causing privacy invasion. In addition, the original data can be stored on the server to maintain availability and can be used for electricity pricing or electricity usage searches.

V. EXPERIMENT AND IMPLEMENTATION

If the data matches the first time it is registered, the verification will indicate success, and if it has been tampered, the verification will report a failure. The transaction does not display the original data. This allows you to meet data integrity, confidentiality, and availability.


Hybrid Cloud

Welcome to Amazon S3 Cloud Service, which offers extensible cloud services with reliable cost with different services.......

Amazon S3 Server

Amazon S3 (Simple Storage Service) is a web service offered by Amazon Web Services. Amazon S3 provides storage through web services interfaces (REST, SOAP, and BitTorrent).[1] Amazon launched S3 on its fifth publicly available web service, in the United States in March 2006[2] and in Europe in November 2007

Fig 8. Hybrid Cloud

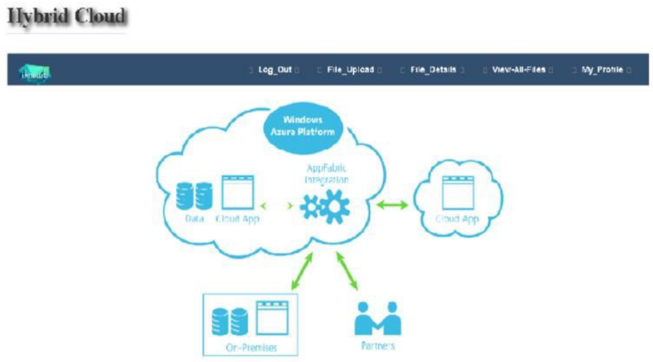
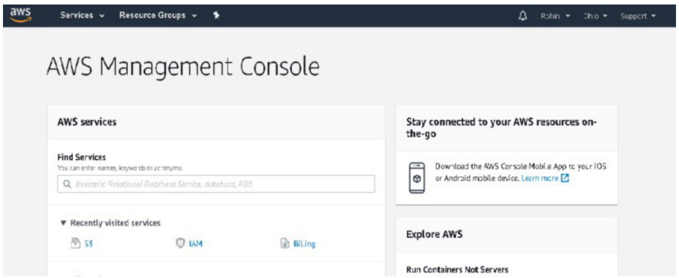


Fig 9. Cloud Architecture



AWS Management Console

AWS services

Find Services
You can enter names, keywords or acronyms.

Example: Relational Database Service, database, RDS

▼ Recently visited services
S3 IAM Billing

Stay connected to your AWS resources on-the-go

Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more

Explore AWS

Run Containers Not Servers

Fig 10. Cloud Console

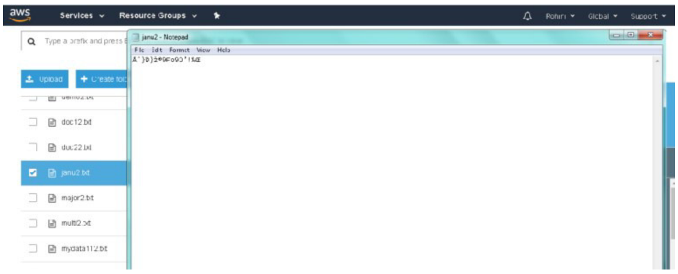


Fig 11. Cloud Data Protection Process

VI. CONCLUSION

In this paper, we contemplated the issue of planning of servers with multi-rest modes for cloud information focuses. The servers can make changes between one dynamic state and distinctive rest states, which includes distinctive rest force and progress delays for the rest modes. We proposed Backtrackand- Update technique to make calendar of the servers, choosing what number of servers in each state ought to be changed to which states in each timeslot, so that the all out force utilization can be limited while fulfilling the QoS prerequisite. The issue is too enormous to be in any way explained by existing strategies, so we isolate the entire issue and afterward overcome them individually while thinking about the progressing changes during the breakpoints. We too consider utilizing DVFS to additionally decrease the vitality brought about by the over provisioned processing limit.

REFERENCES

[1] Gungor, V. Cagri, et al. "A survey on smart grid potential applications and communication requirements." Industrial Informatics, Vol.9, No.1, 2013, pp. 28-42.

[2] Gangale, Flavia, Anna Mengolini, and Ijeoma Onyeji., "Consumer engagement: An insight from smart grid projects in Europe.", Energy Policy, Vol.60, 2013, pp.621-628.

[3] Luan, Shang-Wen, et al. "Development of a smart power meter for AMI based on ZigBee communication", Power Electronics and Drive Systems, 2009. PEDS 2009. International Conference on. IEEE, 2009.

[4] Common Criteria for Information Technology Security Evaluation, Version3.1, CCMB, Setp.2006.

[5] Youngu Lee, A Study for PKI Based Home Network System Authentication and Access Control Protocol, KICS '10-04Vol.35No.4 [6] Kepco, Prosumer Power Trading, http://home.kepco.co.kr

[7] Andreas M, Masteing Bitcoin: Unlocking Digital Cryptocurrencies,