ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing with Blockchain

Arpita Krishna Bhat[1], Prakruthi K[2], Mathiyalagan R[3]

Final Year UG Student, Department of Information Science and Engineering, School of Engineering and Technology Jain University, Bangalore, India[1, 2]

Assistant Professor, Department of Information Science and Engineering, School of Engineering and Technology Jain University, Bangalore, India[3]

ABSTRACT: The cloud administrations have turned out to be mainstream and furthermore have empowered the on-request application arrangement with the ease and furthermore with the flaw tolerant versatile and scalable system. These administrations of the cloud will be offered by the suppliers of the cloud where they use authorization authentication and the accounting framework which is based on the client-server model. Despite the fact that this sort of model has been utilized over a long time the examination demonstrates that it will be powerless for the different hacks and for the end users. With the expansion to it the cloud supplier will have the all-out command over the clients' information or the data where they will trace monitor spill and even they will adjust with their position. Subsequently the client information computerized identity ownership and the utilization of the administration of the cloud have been brought up in protection and the security for the clients' worry. Block chain and the uses of the block chain are contemplated and they are the elective model for the validation approval and bookkeeping and it is proposed dependent on block chain ethereum. Also the model will be created and with which it empowers clients for consuming the cloud benefits this is finished by validating approving and bookkeeping it with the single character without the private client information sharing. Here the tests will keep running with the model for the verification with which it fills in as it is normal. For surveying the adaptability and the achievability of the arrangement the estimations are finished.

KEYWORDS: Block chain, AES Algorithm, SHA 1 Algorithm, Biometric Identification, Aadhar Card.

I. INTRODUCTION

Presently we all are getting to the administrations of the cloud on practically every day schedule for instance, for sharing the data and to be associated with the companions we are utilizing, for the most part, referred to long range interpersonal communication locales, for example, Face book, LinkedIn, and Twitter. We are utilizing the email frameworks, for example, Yahoo, Gmail, Hotmail and numerous others for trading the messages with one another. There are on-request administrations, for example, Netflix, Hotstar, and others to stare at the TV and films. Distributed storage administrations, for example, iCloud, Google Drive and the Drop box will store advanced media, for example, notes, photographs, recordings, and the reports. To lessen operational expense and improve income the cloud administrations are used by the majority of the ventures for conveying their applications and the administrations. For instance, Amazon Web Services is utilized by Netflix to have their administrations, social news site Reddit and the Uber ride-sharing administration are utilizing the Amazon Elastic Compute Cloud (EC2) for giving their administrations. In this way, it will be evident that cloud administrations have turned into a vital piece of business on an ordinary premise. Thus the insurance of clients' information which is put away on the cloud and its security assumes a crucial job, so the biometric assurance is presented.

Biometric security is assuming a significant job in distinguishing the clients. Nowadays everybody is picking the biometric insurance as opposed to the customary techniques for information security. The biometric insurance is

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

increasingly dependable and most advantageous strategy contrasted with all other customary strategies, for example, passwords or recognizable proof cards. The biometric ID is connected in different fields. These fields are by utilizing a unique finger impression, facial examples and iris. All these are gathered from various sensors which are utilized for location dependent on biometric qualities.

II. LITERATURE SURVEY

Proposed novel privacy preserving biometric identification scheme [1] in cloud computing. To realize the efficiency and security requirements, they have designed a new encryption algorithm and cloud authentication certification. The detailed analysis shows that it can be used for resisting the potential attack. Besides, through the performance evaluation, they have further demonstrated that the proposed scheme meets the efficiency need well.

AES-Based Cryptographic and Biometric Security Coprocessor [2] IC in 0.18-µ µµ µm CMOS Resistant to Side-Channel Power Analysis Attacks. Differential routing and WDDL are the techniques that help us to avoid attacks. The results of experiments gave us a result that 1,500,000 acquisitions are not quite enough to show a 128-b key. There is an increase in the tradeoffs three times in area and minimum clock period and four times increase in consumption of power. Even with punishments or fines, the coprocessor spends less energy and faster magnitude than on the primary processor.

A Fingerprint Encryption Scheme Based on Irreversible Function and Secure Authentication [3]. This paper has given us so much information regarding the fingerprint security methods. The irreversible function that has been proposed in this paper helps protect the original template and CRT is used for conjoining the private key with the fingerprint vault that is transformed. The irreversible function guarantees the security after transformation even if system is under attack. The fingerprint encryption system that is proposed in this paper, according to the security analysis shows that the efficiency and security are the higher and complexity is only slightly increased. That is all about the literature survey. All these papers have given us insight for developing this project and are very informative.

SHA 1that is review on Secured Hash [4] Algorithms. This paper gives the details on the brief application, contribution of hash function of this generation and history. In various fields the secure hash functions are applied for providing the secured data transfer and authentication of the messages and other information linked through the series of the algorithms.

Existing System

A. Aadhar Card

Government data are directly sent to the cloud service provider & the assumption is cloud service provider is encrypting & storing the data is not used any block chain & other thing. But it is already proved that our Aadhar card details are hack able and it is hacked & it is already released in the net. This old system format is unsecured.

III. PROPOSED SYSTEM

We propose a capable and security ensuring biometric recognizing evidence redistributing plan. Specifically, the biometric to execute a biometric recognizing confirmation, the database owner scrambles the request data and submits it to the cloud. The cloud performs conspicuous confirmation undertakings over the encoded database and returns the result to the database owner. A cautious security examination exhibits that the proposed arrangement is secure paying little heed to whether attackers can deliver recognizing evidence requests and plot with the cloud. Differentiated and past shows, preliminary outcomes exhibit that the proposed arrangement achieves a redominant execution in both arranging and ID systems.

A. System Architecture

System Architecture setup perceives the general hypermedia structure for the WebApp. Designing arrangement is appended to the targets set up for a WebApp, the substance to be presented, the customers who will visit, and the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

course thinking that has been developed. Content plan based on the manner by which content things and composed for presentation and course. WebApp configuration keeps an eye on the manner by which the application is composed to manage customer joint effort, handle inside getting ready errands, impact course, and present substance. WebApp building is described inside the setting of the headway condition in which the application is to be realized.

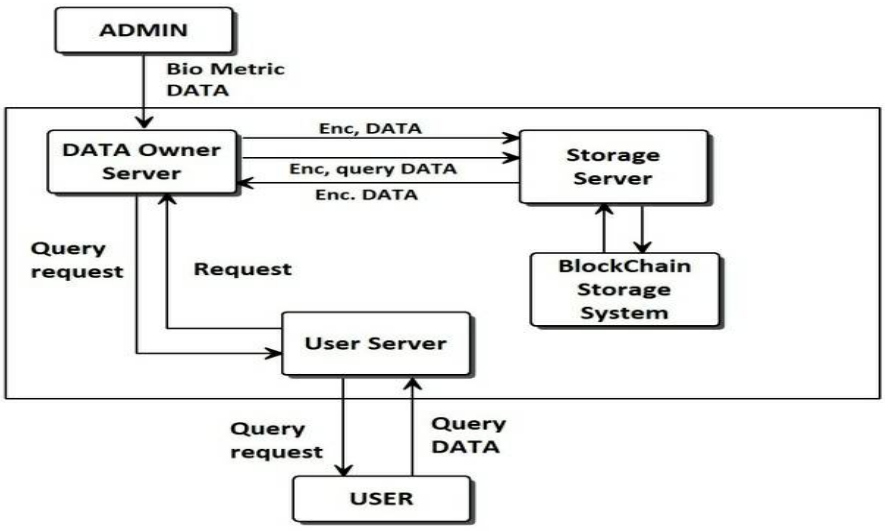

Fig.1. System Architecture

B. System Requirement

B. i. Specification

A Software Requirement Specification (SRS) is fundamentally an association's comprehension of a client or potential customer's framework prerequisites and conditions at a specific indicate earlier any genuine plan or advancement work. The data assembled amid the examination is converted into a report that characterizes a lot of prerequisites. It gives the concise depiction of the administrations that the framework ought to give and furthermore the imperatives under which, the framework ought to work. For the most part, the SRS is an archive that totally depicts what the proposed programming ought to manage without portraying how the product will do it. It's a two-way protection strategy that a guarantee that both the customer and the association comprehend different necessities from that viewpoint at a given point in time.

The SRS report itself states in exact and unequivocal language those capacities and abilities a product framework must give, just as states any required imperatives by which the framework must tolerate. The SRS additionally works as an outline for finishing a task with as meager cost development as would be prudent. The SRS is regularly alluded to as the "parent" report since all consequent task the board records, for example, structure details, explanations of work, programming design determinations, testing and approval plans, and documentation plans, are identified with it. Prerequisite is a condition or capacity to which the framework must acclimate. Necessity Management is a precise methodology towards evoking, sorting out and recording the prerequisites of the framework plainly alongside the relevant properties. The tricky troubles of Requirements are not constantly evident and can emerge out of any number of sources.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

C. Procedure

In our application, we are providing security for aadhar card details with the help of biometrics. Here, we provide an extra layer of protection using the blockchain concept. The first step we do is that the admin uploads the user data and the user will get a conformation mail with the aadhar number and password. Using this password, the user must login in to the system. The user must input the aadhar number and their fingerprint and send a verification request to the admin. Only when the admin verifies that the details are true, will the user be able to access all the details. To achieve this we use AES algorithm, SHA-1 algorithm and fingerprint algorithm.

C.i. AES Algorithm

We use AES algorithm which is significant for protecting the security and opposing assaults on our information. In AES calculation, block length is constrained to 128 bits and the key size can be freely determined to 128, 192 or 256 bits. Key got as info cluster of 4 lines and N_k sections. N_k = 4, 6, or 8, the parameter which depends on the key size. Info key is ventured into a variety of 44/52/60 expressions of 32 bits each. 4 distinct words fill in as a key for each round.

Key size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Number of rounds	10	12	14
Expanded key size (words/byte)	44/176	52/208	60/240

Fig.2 AES key size

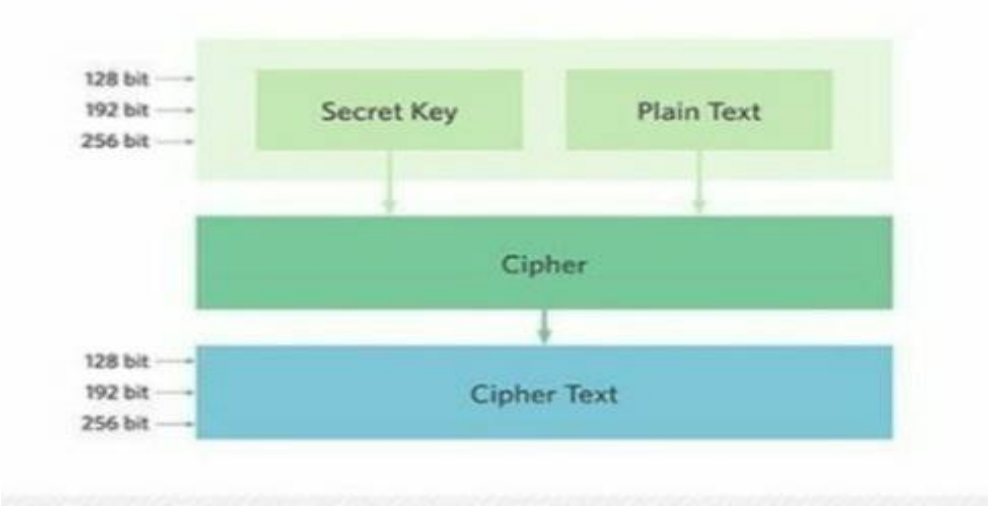

Fig.3 AES key size

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

C.ii. AES Algorithm

SHA-1 different compared to the single bitwise message rotation schedule with the predecessors. In the SHA-1 algorithm the length of the message is padded for 448 mod 512 where the following 64-bit length value is then added to that. Later, 5-word (160-bit) buffer i.e. A, B, C, D, E initialization is done for processing the message in the 16word (512-bit) blocks by accessing 4 rounds of the 20-bit operation on the message block and then on the buffer, later the output is added to the input of the buffer which will yield to the new value of the buffer, and this will be regarded as value of the hash output.

C.iii. Fingerprint Algorithm

Fingerprint algorithm is widely used now-a-days as biometric security has become popular. Here we consider the endpoints, ridges, the direction they move towards and loops are used as parameters. First the fingerprint will be converted to grayscale and then the image will be enhanced and binarized. The resultant image after thinning will be detected pixel-wise for minute features. It is very unlikely that two fingerprints will have the same feature. This is why we have used biometric data as a security measure.

IV. EXPECTED RESULT

Biometric system has different web servers which interact with other server using web server technique. One server is used for admin it accepts client data encrypt and give to cloud service provider web server. The second server is cloud service provider block-chain web server, this server will accept the data from admin server and convert the transaction details into blocks and store it in block-chain storage. The third server is user server which takes the query input client unique ID and his finger print, and this server send the data to admin server, in turn admin server will send the client unique id in hash code format to cloud service provider block-chain web server. When block-chain web server receives the hash code it will retrieve corresponding block from block-chain and send it back to admin server. Admin server extracts the finger print from the received data and it will compare the finger print with query input fingerprint if both are matching it send client data to user web server.

REFERENCES

[1] AES-Based Cryptographic and Biometric Security Coprocessor IC in 0.18-µ µµ µm CMOS Resistant to Side-Channel Power Analysis Attacks Kris Tiri, David D. Hwang, Alireza Hodjat, Bo-Cheng Lai, Shenglin Yang, Patrick Schaumont, and Ingrid Verbauwhede, 2006
[2] An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing by Liehuang Zhu 1, (Member, IEEE), Chuan Zhang1, Chang Xu 1, Ximeng Liu 2, (Member, IEEE), AND Cheng Huang 3 ,2013
[3] A Fingerprint Encryption Scheme Based on Irreversible Function and Secure Authentication, Yijun Yang, Jianping Yu, Peng Zhang, and Shulan Wang, 2015
[4] Brief Review on Journey of Secured Hash Algorithms, by Prof. Santanu Debnath, Dr. Abir Chattopadhyay, Subhamoy Dutta ,2017
[5] ''Security analysis of collusion-resistant nearest neighbour query scheme on encrypted cloud data,'' IEICE Trans. Inf. Syst., vol. E97.D, no. 2, pp. 326–330, by Zhu, T. Takagi, and R. Hu, 2014.
[6] C. Zhang, L. Zhu, and C. Xu, ''PTBI: An efficient privacy-preserving biometric identification based on perturbed term in the cloud,'' Inf. Sci., vols. 409–410, pp. 56–67, Oct. 2014
[7] J. Fournier, S. Moore, H. Li, R. Mullins and G. Taylor, "Security Evaluation of Asynchronous Circuits," CHES, pp. 137-151, 2003.
[8] N. Pramstaller, F. Gürkaynak, S. Häne, H. Kaeslin, N. Felber, and W. Fichtner, "Towards an AES Crypto-chip Resistant to Differential Power Analysis," ESSCIRC, pp. 307-310, 2004