A Centralized Data Validation Approach For Distributed Healthcare Systems In Dew-Fog Computing Environment Using Blockchain

Grace Simpson[1, 2], Kester Quist-Aphetsi[1,2,3]
[1]Computer Science Department, Ghana Technology University College, Ghana
[2]Cyber Security Division, CRITAC, Ghana
[3]Directorate of Information Assurance and Intelligence Research, CRITAC, Ghana

gsimpson@gtuc.edu.gh, kquist-aphetsi@gtuc.edu.gh

***Abstract*— Patients healthcare data should be securely available and accessible to authorized users when needed to facilitate healthcare professionals to make a decision regarding patients. Data from dew systems should be synchronized with the data in the cloud when there is connectivity. Validation of data from the dew system should be done by the cloud server to ensure patients data integrity. This paper proposes an adoption of a framework that validates centralized data for distributed healthcare systems in a dew-fog computing environment using tiger hash function to provide integrity to patient data.**

Keywords- cloud computing, dew computing, fog computing, blockchain, centralized data, tiger hash functions

I. INTRODUCTION

Healthcare data about patients should be reliable and available to patients' primary healthcare provider and other healthcare facilities on demand especially in emergency cases where patients have to be treated outside of their primary healthcare facilities. According to Hassan et al [1], patient healthcare records will exceed tens of millions by end of 2017 bringing the need of putting in place secure data storage infrastructure capable of processing data in parallel, and fault-tolerant mechanism of high availability. Healthcare providers keep patient's data locally at facilities accessible only to that facility. Patient referrals to different health centers require new generation of patient data which in turn is confined to the new premises. A centralized repository of patient data will help solve the risk associated with conflicting treatments provided by different healthcare providers to same patient[2], at the same time, patient healthcare data is sensitive and should be protected from unauthorized access. This paper proposes a framework to centralized patient data in a dew-fog environment, which will be validated using the tiger hash function stored over distributed systems.

II. LITERATURE REVIEW

A. CLOUD COMPUTING

The cloud computing model allows access to a shared pool of configurable computing resources which includes network, servers, storage, applications, and services which is delivered over the internet [3], [4]. The main objective of cloud computing is to enhance the use of distributed resources, combining them to achieve higher throughput in order to solve large-scale computational problems, which offers customers the flexibility of non-payment for infrastructure, its installation, required work force to handle such infrastructure and maintenance [5]. NIST categorized five (5) attributes of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service [5], [6]. Shared architecture, metering architecture, disaster management, green computing, uninterrupted services, cost reduction and easy management, and lower IT barriers to innovation are some advantages listed by past research [5]–[7]

B. FOG COMPUTING

Fog computing works by bringing together the underlying network and network resources at the edge of the network by allowing services to be hosted at the end devices or access points, this enables the virtualized platform to provide storage, network services, and computational power amongst end devices [8]. Fog computing incorporates cloud computing, and services to the edge of the network. Fog computing is differentiated from cloud computing using the proximity to end-users, the dense geographical distribution and mobility support [9]. [9], [10] identified smart grid, smart traffic lights and connected vehicles, wireless sensor and actuator networks, decentralized building control, augmented reality and real-time video analytics, content delivery and caching and mobile big data analytics as application areas in fog computing. Dastjerdi and Buyya [11] identified that, the many nodes involved in fog computing causes less energy efficient management. Trust, authentication, secure

978-1-7281-7417-4/19/$31.00 ©2019 IEEE
DOI 10.1109/ICSIoT47925.2019.00006

communications, end user's privacy and malicious attacks are other challenges identified by Mukherjee *et al.* [12].

C. DEW COMPUTING

Dew computing (DC) presents a user the possibility of accessing user information in the absence of Internet connectivity[13]. Wang[14] in his paper identified independence and collaboration as two key features of DC. Dew computing has the ability to self-heal, self-adapt and transparency as some key advantages [13].

D. BLOCK CHAIN

Blockchain technology proposed by Nakomoto [15] is a growing list of record blocks linked using cryptographic hash that has a time stamp that records transactional data. Since the introduction of blockchain, researchers have introduced or proposed a number of application areas possible to incorporate blockchain technology which includes healthcare.

III. METHODOLOGY

A. SYSTEM ARCHITECTURE

By the use of blockchain, patient digital data can be generated, transferred, exchanged amongst health facilities and protected from illegal duplication and counterfeiting [16] Figure 1. shows how the proposed system works to share healthcare data from the centralized data center with the different healthcare facilities. The proposed system will validate data exchange and reconcile records coming from different facilities databases H_1, H_2, ……H_n. Each database has a corresponding date of new records that will be sorted based on the chronological order that the healthcare data arrived at the centralized center B.

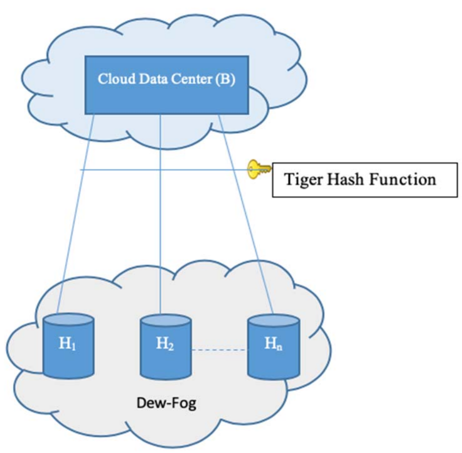

Figure 1. Dew-Fog Architecture. Source: Authors construct 2019.

The dew-fog environment enables facilities to work with data even when the Internet service is unavailable for a period of time, after which a synchronization takes place to update the records to the centralized location. Before data is synchronized the tiger hash is used to secure and validate the data before committing into the cloud data center.

B. TIGER HASH

Tiger hash function (THF) is an iterative hash function designed to process 512-bit input message blocks to produce a 192-bit hash function value. It is fast and secure cryptographic function that efficiently work on 32-bit and 64-bit machines [17]. TFH was designed based on the Merkle-Damgàrd paradigm which operates on a 64-bit word maintaining 3 words of state processes 8 words of data, applicable normally in file sharing networks.

TIGER HASH SPECIFICATION

INITIALIZATION STAGE:

Three 64-bit registers called a, b, c as the intermediate hash function values are initialized to h_0, where

$$a = 0x0123456789ABCDEF$$
$$b = 0xFEDCBA9876543210$$
$$c = 0xF096A5B4C3B2E187$$

Each successive 512-bit message block is divided into eight 64-bit words $x0, x1, \ldots \ldots x7$ and a computation is performed to update h_i to h_{i+1}.

COMPUTATION STAGE:

In the computation stage, three passes are done with a key schedule between each pass; an invertible transformation of the input data which prevents an attacker forcing sparse inputs in all three rounds.

FEEDFORWARD STAGE:

Finally a feedforward stage in which the new values of $a, b, and\ c$ are combined with their initial values to give h_{i+1}:

save_abc -------------------------(1)
pass $(a, b, c, 5)$ -------------------------(2)
key_schedule -------------------------(3)
pass $(c, a, b, 7)$
key_schedule
pass $(b, c, a, 9)$
feedforward -------------------------(4)

(1) save_abc saves the values of h_i

$$aa = a;$$
$$bb = b;$$
$$cc = c;$$

(2) pass (a, b, c, mul) is

$round(a, b, c, x0, mul);$

$round(b, c, a, x1, mul);$

$round(c, a, b, x2, mul);$

$round(a, b, c, x3, mul);$

$round(b, c, a, x4, mul);$

$round(c, a, b, x5, mul);$

$round(a, b, c, x6, mul);$

$round(b, c, a, x7, mul);$

Where
$round(a, b, c, x, mul)$ is $c \,\hat{}= x;$
$a -= t, [c\_0] \hat{} t2[c\_2] \hat{} t3[c\_4] \hat{} t4\,[c\,\_\,6];$
$b += t4\,[c\,\_\,1]\, \hat{}\, t3\,[c\_3]\, \hat{} t2[c\_5] \hat{} t1[c\_7];$
$b *= mul;$
And where c_i is the ith byte of $c(0 \leq i \leq 7$

(3) Key_Schedule is
$x0 -= x7 \hat{} 0xA5A5A5A5A5A5A5A5;$
$x1 \,\hat{}= x0;$
$x2 += x1;$
$x3 -= x2 \,\hat{}\, ((\sim x1) \ll 19);$
$x4 \,\hat{}= x3;$
$x5 += x4;$
$x6 -= x5 \,\hat{}\, ((\sim x4) \gg 23);$
$x7 \,\hat{}= x6;$
$x0 += x7;$
$x1 -= x0 \,\hat{}\, ((\sim x7) \ll 19);$
$x2 \hat{} = x1;$
$x3 += x2;$
$x4 -= x3 \hat{} ((\sim x2) \gg 23);$
$x5 \hat{} = x4;$
$x6 += x5;$
$x7 -= x6 \hat{} 0x123456789ABCDEF;$

Where $\ll and \gg$ are logical shift left and right operators.

(4) Feedforward is

$$a \hat{} = aa;$$

$$b -= bb;$$

$$c += cc;$$

The resultant registers a, b, c are the 192 bits of the hash value h_{i+1}

IV. RESULTS

In Figure 2 and Figure 3 below, the first column represents number of individual patients assessing hospitals 1 and hospital 2 respectively, patient ID is in column 1, data generated is in column 2 and the corresponding time and hash value of the data is given in columns 3 and 4 respectively.

1 , 13821 , 09:03:40am , 0abfaa47af31d857cbc99134aec89d7d
2 , 00361 , 12:14:47pm , 57e7a847daaf4681fbfb0130aed841b0
3 , 68297 , 05:10:53am , 5fbc4aea38ddd776811bf9d75b0123c5
4 , 45100 , 09:50:45am , 55caf73b02e4ad4535c25549f3e53a2c
5 , 46454 , 12:17:01am , ee011e1ae645fa11111ad9435cb71f61

Figure 2: Hash Values from Hospital 1

1 , 93787 , 09:48:53pm , 7e4a7f497d00d469fd4bb9e6322deda4
2 , 15301 , 03:54:07pm , c61175d6abbbb66f3ab5a68d9740d451
3 , 38513 , 06:05:16am , 116ac1e88cf944fe1c236ff52565f66e
4 , 17366 , 01:15:36am , 5eac0abc7751853edc6c02a31a20f6a8
5 , 12522 , 04:33:00am , fcce5d4282fcd0dcb3d8b2c58a0457e4

Figure 3: Hash Values from Hospital 2

Data synchronization with centralized data Center B, is done from hospitals 1 and hospital 2 depicted by databases H_1 and H_2 in Figure 1. The patient data is sorted based on the timestamp on each record and rearranged to reflect current data which is committed to the cloud for storage as depicted in Figure 4 below.

1 , 2 , 00361 , 12:14:47pm , 57e7a847daaf4681fbfb0130aed841b0 , 12:14:47pm , cc80146d85be6ee87f446f33c4e7e0b5
2 , 5 , 46454 , 12:17:01am , ee011e1ae645fa11111ad9435cb71f61 , 12:17:01am , b1988f7a201c5a73cbf2839ba1d4b241
3 , 3 , 68297 , 05:10:53am , 5fbc4aea38ddd776811bf9d75b0123c5 , 05:10:53am , ef085703b7b184a918ee348588dd6c44
4 , 4 , 45100 , 09:50:45am , 55caf73b02e4ad4535c25549f3e53a2c , 09:50:45am , 1c82356ecba2e7c7179065528be597f5
5 , 1 , 13821 , 09:03:40am , 0abfaa47af31d857cbc99134aec89d7d , 09:03:40am , 061d5de69008ec2869c6af5a8284d483
6 , 5 , 12522 , 04:33:00am , fcce5d4282fcd0dcb3d8b2c58a0457e4 , 04:33:00am , 75bb9f72671b306a0a3b43831e9da98a
7 , 3 , 38513 , 06:05:16am , 116ac1e88cf944fe1c236ff52565f66e , 06:05:16am , 9bd1716ab10f91b0eb862d19e03eaee1
8 , 4 , 17366 , 01:15:36am , 5eac0abc7751853edc6c02a31a20f6a8 , 01:15:36am , db1b8a408a0bff5caf2fdff2eba101b6
9 , 2 , 15301 , 03:54:07pm , c61175d6abbbb66f3ab5a68d9740d451 , 03:54:07pm , 74bde6d8ed7ee6bf25bb36324a895fd7
10 , 1 , 93787 , 09:48:53pm , 7e4a7f497d00d469fd4bb9e6322deda4 , 09:48:53pm , 8980cb3a05578474f2085020aee8a3d8

Figure 4: Hash Values from Hospital 1 and Hospital 2

V. CONCLUSION

The paper proposes a framework that offers an easy way of ensuring patients healthcare data is available at different health care facilities. The use of the blockchain ledger allows the use of timestamp for the databases to verify and store current patient health information to the cloud of centralized data. The hashes generated ensured that the data was validated and protected from tampering. This research has provided a secure means of validating and transmitting sensitive health data for use across multiple health facilities from a centralized location.

ACKNOWLEDGMENT

My profound gratitude to my head of department Dr. Kester Quist-Aphetsi for his patience and guidance in my academic writing.

REFERENCES

[1] M. K. Hassan, A. I. El Desouky, S. M. Elghamrawy, and A. M. Sarhan, "Big Data Challenges and Opportunities in Healthcare Informatics and Smart Hospitals," no. November, pp. 2–26, 2019.

[2] A. S. Y. Adu, F. Twum, J. B. Hayfron-Acquah, and J. K. Panford, "Cloud Computing Framework for E-Health in Ghana: Adoption Issues and Strategies: Case Study of Ghana Health Service," *Int. J. Comput. Appl.*, vol. 118, no. 17, pp. 13–17, 2015.

[3] B. Snaith, M. Hardy, and A. Walker, "Emergency ultrasound in the prehospital setting: The impact of environment on examination outcomes," *Emerg. Med. J.*, vol. 28, no. 12, pp. 1063–1065, 2011.

[4] D. C. Utz and M. F. Buscemi, "Extragonadal testicular tumors.," *J. Urol.*, vol. 105, no. 2, pp. 271–274, 1971.

[5] Y. Jadeja and K. Modi, "Cloud computing - Concepts, architecture and challenges," in *2012 International Conference on Computing, Electronics and Electrical Technologies, ICCEET 2012*, 2012, no. November, pp. 877–880.

[6] S. Bera, S. Misra, and J. J. P. C. Rodrigues, "Cloud Computing Applications for Smart Grid: A Survey," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1477–1494, 2015.

[7] M. G. Avram, "Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective," *Procedia Technol.*, vol. 12, pp. 529–534, 2014.

[8] M. Aazam and E. N. Huh, "Fog computing and smart gateway based communication for cloud of things," in *Proceedings - 2014 International Conference on Future Internet of Things and Cloud, FiCloud 2014*, 2014, no. October 2016, pp. 464–470.

[9] I. Stojmenovic and S. Wen, "The Fog Computing Paradigm: Scenarios and Security Issues," in *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems*, 2014, vol. 2, pp. 1–8.

[10] S. Yi, C. Li, and Q. Li, "A Survey of Fog Computing," in *Proceedings of the 2015 Workshop on Mobile Big Data - Mobidata '15*, 2015, no. June 2015, pp. 37–42.

[11] A. V. Dastjerdi and R. Buyya, "Fog Computing: Helping the Internet of Things Realize Its Potential," *Computer (Long. Beach. Calif).*, vol. 49, no. 8, pp. 112–116, 2016.

[12] M. Mukherjee *et al.*, "Security and Privacy in Fog Computing: Challenges," *IEEE Access*, vol. 5, pp. 19293–19304, 2017.

[13] P. P. Ray, "An Introduction to Dew Computing: Definition, Concept and Implications," *IEEE Access*, vol. 6, pp. 723–737, 2017.

[14] Y. Wang, "Definition and Categorization of Dew Computing," *Open J. Cloud Comput.*, vol. 3, no. 1, pp. 1–7, 2016.

[15] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system, Oct. 2008," *URL http//www. bitcoin. org/bitcoin. pdf.(cited pp. 15 87)*, 2017.

[16] T. Aste, P. Tasca, and T. Di Matteo, "Blockchain Technologies: The Foreseeable Impact on Society and Industry," *Computer (Long. Beach. Calif).*, vol. 50, no. 9, pp. 18–28, 2017.

[17] R. Anderson and E. Biham, "Tiger: A fast new hash function," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 1039, pp. 89–97, 1996.