Enhancing Privacy for Big Data in Healthcare Domain based on Cryptographic and Decentralized Technology Methods

Tahir Yinka, Olaosebikan, Su-Cheng Haw, Gaik-Yee Chan

Abstract*: Privacy is one of the biggest concerns that hinder most organizations to adopt the Big Data technology. Some mechanisms and systems have been set-up to handle huge databases. Nevertheless, the scalability requirements of Big Data are far beyond the conventional databases to handle. Therefore, it is trivial to set-up scalable privacy algorithms for conventional databases. Most data are stored in a single location, which means the records it keeps are open and effortlessly irrefutable to third parties. Centralized versions of this data make it too easy for hackers to attack. As such, in this paper, we present the opportunities and challenges of implementing cryptography and blockchain for privacy perseverance in Big Data, focusing in the healthcare domain. In addition, we also present some use cases of integrating Directed Acyclic Graph (DAG) into healthcare database framework for anchoring information security and privacy.

***Index Terms*: Big Data, Cryptography, Symmetric Encryption, Directed Acyclic Graph, Blockchain, IOTA.**

I. INTRODUCTION

In the Big Data era, data is always being gathered and investigated, prompting financial development [1]. For the most part, huge information can be characterized "as the Information asset characterized by such a high volume, velocity and variety to require specific technology and analytical methods for its transformation into value" . As part of big data, multimedia is progressively getting to be the "Biggest big data" as it as of now creates 60% of Web movement also, 70% of cell phone activity. Specialists evaluated that by 2020, Internet of Things (IoT) innovation will be incorporated into 50 billion items [2]. Big Data differences are cited in terms of velocity, volume, and variety of data [3] is because of the exponential growth.

Numerous protection or security frameworks have been proposed in [2], [3] and [4] to safeguard security in the correspondence channels for gadgets generating Big Data. Cryptography is the most known procedure for guaranteeing security and protection of the data by encryption [4]. It is important to propose an encryption procedure which is suitable for Big Data. Generally, encryption techniques are categorized into two main groups, which are symmetric encryption, and asymmetric encryption techniques [4]. Symmetric encryption technique is more suitable to cloud storage because it encrypts large volume data in minimum time duration. For instance, Homomorphism encryption is one of the symmetric encryption, which enables cloud service providers to execute calculations on ciphered data put away in the cloud without any knowledge of private keys [5]. On the other hand, Paillier homomorphic is one of the asymmetric encryption to determine, indicate interest in encrypted banking dataset.

The first account of the web is one of the radical decentralizations and opportunity. Amid the most recent decade, the web's staggering development was combined with expanded centralization. Hardly any expansive organizations presently claim imperative points of the web, and therefore a great deal of the information made on the web (big data). The absence of straightforwardness and command over these associations uncovers the negative parts of centralization [6]. Centralized organizations both open, and privates collect expansive amounts of individual and classified data. Individuals have practically zero commands over the information that is put away about them and how it is utilized.

A Big data revolution is in progress in social insurance such as healthcare. Begin with the rapid expanded supply of data [7], for example, The US social insurance framework is quickly receiving electronic healthcare records, which will significantly build the amount of clinical information that are accessible electronically [8]. While the healthcare services industry saddles the intensity of Big data, security and privacy issues are at the point of convergence as rising dangers and vulnerabilities keep on developing.

II. LITERATURE REVIEW

Cryptographic strategies are grouped into two, namely the symmetric encryption, and asymmetric encryption.

A. Symmetric Encryption

Symmetric encryption calculations are calculations for cryptography that utilization the equivalent cryptographic keys for encryption of plaintext and decrypting of ciphered text. The keys might be indistinguishable, or there might be a straightforward change to go between these two keys. Some symmetric encryption

Revised Manuscript Received on August 18, 2019

Tahir Yinka, Olaosebikan, Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Malaysia.
Su-Cheng Haw, Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Malaysia.
Gaik-Yee Chan, Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Malaysia.

algorithm schemes include:

1) The Attribute-Based Encryption Approach [10]: In this approach, key creation for the clients is issued by discrete key creation specialist, and characteristics of the clients will be overseen by property administration expert. Private keys for the clients will be produced dependent on the qualities of the clients. The proposed approach helps to comprehend enormous computational expense caused by utilizing the symmetric encryption calculation to guarantee the protection of interactive media huge information in the web of Things. Fig. 1 shows the architecture diagram of the approach.

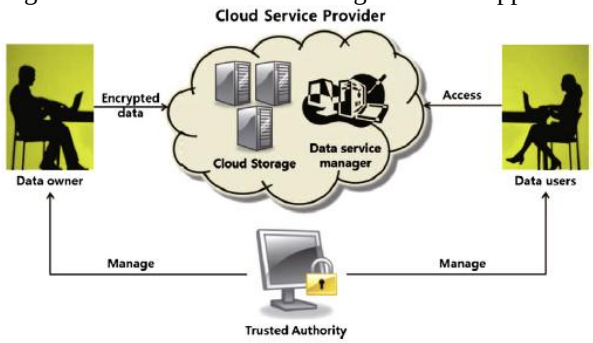

Fig. 1. Architectural description of a cloud storage system [10]

The framework comprises of the accompanying four elements:

a) Trusted specialist: A key generation focus with full trust of all members of the framework. The believed expert gives the essential key materials to this framework by creating open parameters and the ace private key.

b) Cloud specialist organization: This is the information stockpiling the supplier to users that stores the information content redistributed by the information proprietor. This information is accessible and downloadable to expected collectors who have adequate qualifications.

c) Data proprietor: An information stockpiling the user who needs to transfer its information content namelessly to the distributed storage framework after encryption. The encrypted information can be imparted to expected collectors who have adequate accreditations as indicated by the information proprietor.

d) Data Client: This is an outsider distributed storage supporter which sends questions to the specialist organization for encrypted information in the distributed storage framework by utilizing an alias the information proprietor.

In relation to healthcare, proposed scheme enables the patient to share safely their personal health records with clients from various security areas. This is on account of the access policy under which the information is encoded can contain characteristics issued from various trusted parties [10]. However, system still lacks low security level in data storage and data sharing.

2) The Attribute-Based Encryption Approach [10]: Aljawa proposed an asset effective encryption framework for scrambling multimedia enormous information in IoT, by exploiting the Feistel Encryption Plan, Advanced Encryption Standard (AES), and hereditary calculations. The proposed approach has the most reduced running time contrasted with another encryption. Fig. 2 depicts the framework of the proposed approach.

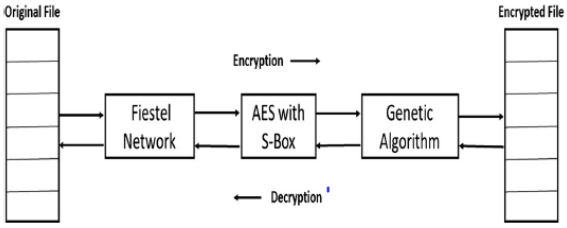

Fig. 2. The framework of resource-efficient encryption system [2]

The proposed framework system comprises of three principal parts: Feistel organizes, AES with S-box, and Genetic algorithm.

a) The Feistel arrange segment partitions the way too little squares and plays out a progression of a move and turn tasks on them. The Feistel arrange produces a figure key that will be utilized in AES part.

b) AES with S-box acknowledges the plaintext and the figured key as info. AES utilizes the Substitution-change arrange and performs 10 rounds of encryption to create the Figured content.

c) The genetic calculation utilizes two levels of mixes: hybrid and change. In the hybrid, a part of the encrpted text and encryption key are swapped, where in Change, a randomly picked bit is flipped in both figured encrpted text and encryption key.

While standard encryption techniques provide a secure solution but are not practical for secure Electronic Health Record (EHR) storage. For instance, AES is usually efficient but introduce complexity in EHR systems as additional mechanisms are required to apply access control. In particular, all healthcare providers use one shared key for encryption and decryption. That is, if the shared key is compromised, all EHRs are compromised [9].

B. Asymmetric Encryption

Asymmetric encryption utilizes a couple of open keys and a private key to scramble and unscrambles messages during computation. Asymmetric encryption takes generally additional time than the symmetric encryption. Some Asymmetric encryption calculation plans are as follows.

1) The Cloudlet-based healthcare system approach [11]: This plan used the adaptability of cloudlet to construct a medicinal services framework and proposes a framework for security assurance, information sharing, and interruption recognition framework to tackle the accompanying issue: (i) Healthcare information security assurance and sharing information, (ii) to create viable countermeasures to keep the medicinal services database from being barged in from outside.

This was accomplished by grouping information using the Number Theory Research

Unit (NTRU) technique to encode a client's body information gathered by wearable gadgets. Proposed scheme assesses the calculation and depict the progressions, conveyance proportion of customer information encryption strategy with remote cloud encryption component being augmented with time.

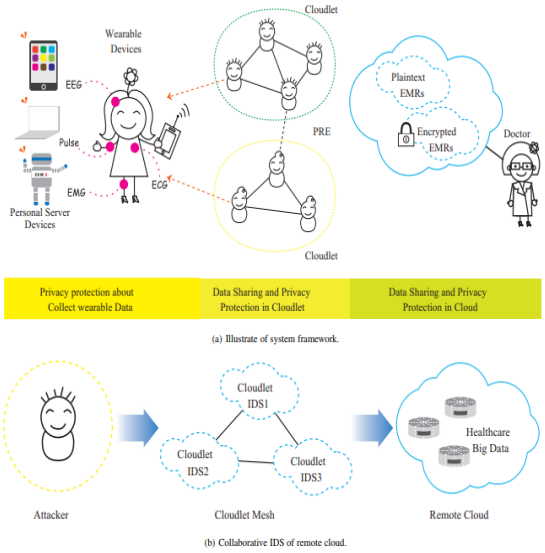

Fig. 3. Cloudlet-based healthcare system [11]

How the issue was tackled is shown as follows.

a) Client information encryption: The framework utilized a completely homomorphic encryption calculation, an open key encryption framework (Asymmetric encryption) to shield the customer's physiological information from being spilled or manhandled.

b) Cloudlet based information sharing: acquire clients' trust levels, and a limit is set for the examination.

c) Remote cloud information security insurance: ensure the information containing clients' touchy data.

Complete homomorphic encryption allows calculation on encrypted information specifically in the cloud without the need to take the information back to the computational hub. However, the expense of performing re-encryption is restrictively high which makes proposed FHE not sufficient.

2) The vertical partitioning and integrity checking of medical dataset approach [12]: This plan proposed an answer that utilizes Symmetric and public key encryption calculation by encoding the information utilizing proficient symmetric key cryptography. This key is thus encoded with the beneficiary's open key, so it must be utilized by the approved clients by the information proprietor. Along these lines, the benefits of the two calculations can be utilized.

This plan utilized four noteworthy segments, which are, (i) Vertical information parcel for medicinal information distributing, (ii) Information converging: for access to medical dataset, (iii) Dataset honesty level check, and (iv) Hybrid Search over encrypted and decrypted data, where by measurable examination and cryptography are utilized together to give numerous standards of harmony between use of restorative information and security insurance. Fig. 4 shows the framework of the proposed approach.

a) Vertical information segment: It segments the first information record table into three tables, i.e., a plaintext table with the properties of medicinal data, an anonymized table with the qualities of semi identifiers, and an encoded table with the traits of unequivocal identifiers and semi identifiers. After this progression, these three tables are put away independently in the cloud.

b) Information consolidating: This segment is used by the information beneficiary to accomplish the dataset-level therapeutic information get to with the approval of the information proprietor; the information beneficiary can get too specific for medicinal information inquiry or examination.

c) Respectability checking: The information proprietor and information beneficiary use this segment to guarantee the put-away information in the cloud is the equivalent as it was the point at which it was initially recorded. The information beneficiary uses this part to understand the record-level medicinal information get to, i.e., to discover one or different intrigued electronic medical records (EMR) in the common restorative dataset. A crossbreed seeks the approach is given to consolidating the scrambled and plaintext scans strategies for the usage of the data recovery over the remote therapeutic information stockpiling.

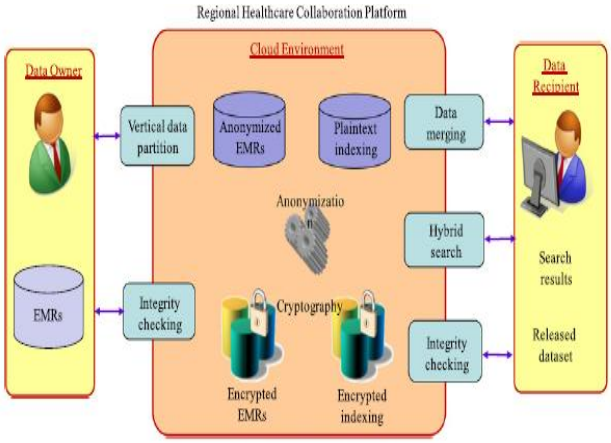

Fig. 4. The framework of the privacy- preserving data storage and sharing [12]

Some other reviewed cryptographic algorithms are shown in Table 1. From Table 1, one can observed that cryptographic methods for securing healthcare dataset provides security assurances depending on approach used, moreover some approaches incurs a very high computational power and depend on some central authority to ensure security measures.

III. DECENTRALIZED APPROACHES

In this section, we will discuss two main decentralized technologies, namely Blockchain and Directed Acyclic Graph (DAG).

Table 1. Summary of the cryptographic approaches

Scheme	Summary of Methods Used		
	Algorithms	*Advantage*	*Disadvantages*
Symmetric Encryption Algorithm [4]	Symmetric	Proposed solution helps users as well as cloud service providers to trust and improve the usage of cloud computing environment.	SEA encrypts whole data to be stored in the cloud storage hence increases computation, encryption and decryption time
Probabilistic public key [13]	Symmetric	Probabilistic approach is suitable for verifying the integrity of data.	High computation and communication time.
Homomorphic encryption [12].	Symmetric	Provides adaptable medical restorative information getting to with various thought about the data use and security assurance	Solution depends on a central authority which is trusted but curious.
SA-EDS, [14]	Symmetric	Evaluations had demonstrated that the proposed plan could adequately guard real dangers from cloud-side.	Proposed scheme lacks secured data duplications which reduce the level of data availability as any of data center down will cause the disappointment of information recovery.
Lightweight homomorphic [15]	Symmetric/ asymmetric	Attains the respectability of shared information and looking resultant information.	Access control challenges are faced by proposed scheme.

A. Blockchain

Blockchain is "a developing rundown of records, called blocks, which are connected utilizing cryptography. Each block contains a cryptographic hash of the past block, a timestamp, and exchange information". Blockchain innovation empowers a decentralized and appropriated condition with no requirement for a central authority. Zyskind et al. [1] furnished a diagram on Blockchain innovation with an accentuation on its application in huge information (Big Data) and mechanical applications as depicted in Fig. 5.

The Blockchain unravels evidence of ownership by means of a crypto-secure, conveyed the record of a sequentially requested transaction. The Blockchain transactions are matched up over the system, framing a worldwide log of what and (generally) when the transactions occur.

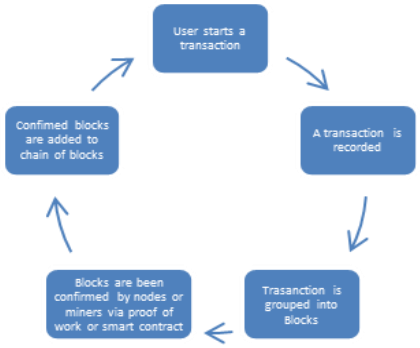

Fig. 5. Blockchain validation and formation

1) The Fine-grained Access Control Approach [1]: This system proposed a Blockchain solution addressing privacy issues on Information Proprietorship, Information Straightforwardness, and Audibility. Fine-grained access control to guarantee application clients claim and control their information without trading off security or restricting organizations' and specialists' capacity to give customized administrations. The proposed solution depends on the Blockchain being alter free, a suspicion that requires an adequately extensive system of untrusted peers. What's more, the arrangement accepts that the client deals with his keys in a protected way, for instance utilizing a safe unified wallet benefit as depicted in Fig. 6.

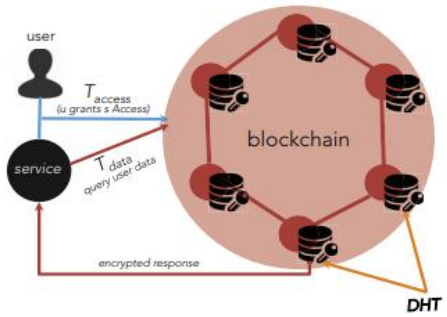

Fig. 6. The Fine-grained Access Control Framework [1]

To additionally clarify over this plan, consider a client introduces an application that utilizes the Blockchain stage for safeguarding his protection. As the client agrees to accept the first run through, another common (client, benefit) personality is created and sent, alongside the related authorizations, to the Blockchain in a Taccess exchange. Information gathered on the telephone (e.g., sensor information, for example, area) is scrambled utilizing a common encryption key and sent to the Blockchain in a Tdata exchange, which along these lines' courses it to an off-Blockchain Data Hash Table (DHT) key-esteem store, while holding just a pointer to the information on people in general record (the pointer is the SHA-256 hash of the information.).

2) The Crowd Sensing Incentive Mechanism Approach [16]: This plan proposed a protection safeguarding Blockchain based secure group detecting motivating force system, by utilizing a hub participation security assurance technique in Blockchain to ensure client protection, in which evident information characteristics assessment by mineworkers can dispense with the security and protection issues caused by a central authority.

This framework comprises of a server and set of partaking Clients, beneath is the Detecting forms (see Fig. 7):

- Server S distributes the detecting task with stores.
- Component of U signified by the client transfers detecting information.

- Data quality checked by miners.
- Transactions checked by miners.
- The server pays some specific measure of remuneration.

Guaranteeing mineworkers security, an exchange confirmation display dependent on hub collaboration technique is utilized, the check procedure I isolated into two sections i.e. intragroup arrangement and Gathering transaction confirmation.

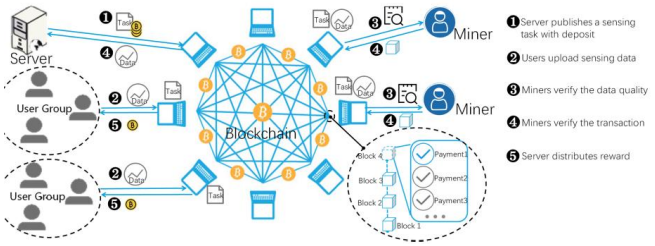

Fig. 7. Proposed solution Blockchain framework [16]

Blockchain would guarantee persistent accessibility and access to continuous information. Ongoing access to information would enhance clinical consideration coordination and enhance clinical consideration in crisis medicinal circumstances. Constant information would likewise enable specialists and general well-being assets to quickly distinguish, detach and drive change for natural conditions that affect general well-being. For instance, plagues could be distinguished before and contained.

Blockchain technology provides individuals, companies and governments with infinite opportunities, which has led to startups of researches and developments such as field of authentication management using a public/private key cryptography, identity management and cryptocurrency use cases. Table 2 depicts summary of related researches/projects with cryptocurrency use cases.

Table 2. Blockchain and Cryptocurrency Use Cases

Scheme	Summary of Blockchain and Cryptocurrency use cases			
	Description	Cryptography Algorithms	Block chain	Cryptocurrency
My Data [19]	This solution provides a self-sorverien and Authentication scheme, in conjuction with Sorvin[].	Public Key Cryptography	Hyper ledger .	No
CertCoin [20]	A completely public and auditable solution based on NameCoin, provides a decentralized authentication system.	Public Key Cryptography for on-line and ofline storaage.	Hyper ledger	Bitcoin
FHIRChain [21]	Provides a token based model to securely share clinical data.	Public/ Private key cryptography mechanism called “Sign then encrypt”.	Ethereum	No
HIE of one [22]	Health Information Exchange of one uses blockchain to shift trust issues role away from healthcare providers by using blochchain to physician credentials and paicient ID.	Public/ Private key cryptography .	Ethereum/ Bitcoin	Bitcoin

B. Directed Acyclic Graph (DAG)

IOTA (DAG crypto currency) is a revolutionary new transaction settlement and data transfer layer for the IoT. Some of the key benefits of IOTA technology are as follows:

- Scalability: The increase in the number of transactions implies a stronger network and confirmation rates get better.
- Decentralization: No miners, every transaction maker is as well a Transaction validator, every transaction maker actively participates in the consensus.
- No transaction fees
- Quantum computing protection.

1) IOTA Structure (T-angle Directed Acyclic Graph): The T-angle succeeds the blockchain as its next transformative advance, as a rule, a T-angle-based digital money (IOTA) works in an accompanying way. Rather than the worldwide blockchain, there is a DAG that we call the T-angle (see Fig. 8). The transactions issued by nodes comprise the site set of the T-angle diagram, which is the record for putting away transactions [17].

The edge set of the T-angle is acquired as follows: when a fresh transaction arrives, it must endorse two past transactions. These endorsements are spoken to by coordinated edges. In the event that there is certainly not a coordinated edge between transaction A and transaction B, yet there is a coordinated way of length no less than two from A to B, we say that A by implication supports B. There is likewise the "Genesis" transaction, which is endorsed either directly or in an indirect way by every other exchange.

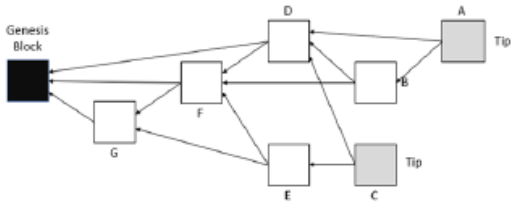

Fig. 8. The structure of the T-angle [17]

2) T-angle DAG Benefits compared to Blockchain for healthcare Applications: To more readily comprehend why IOTA T-angle innovation might be suitable in healthcare domain, we depict the key advantages or near points of interest of IOTA.

The first key advantage of IOTA T-angle is decentralization. The Blockchain system gives prizes to the nodes, as an impetus to repay the computational expense related with "mining" blocks and confirming transactions [18]. IOTA has no ‘’miners’’ or ‘’Mining nodes’’ every transaction maker is a transaction validator, at the point when a new transaction arrives, it must validate two past transactions. These validations are represented by coordinated edges, as appeared in Fig. 8. In this way, IOTA T-angle is reasonable for applications where autonomously human services partners e.g., healthcare centers wish to work together with each other without relying upon some mining expert or nodes.

Secondly, scalability in T-angle is an advantage over blockchain. Speed limitation may constrain the adaptability of blockchain-based applications because of high truncation time. For instance, with the proof of-work convention, there are around 288 000 transactions every day or about 3.3 exchanges every second, all things considered for Bitcoin because of the required calculation remaining task at hand [18]. While in IOTA T-angle, the increase in number of transactions implies a stronger network and confirmation rate get better, which is a necessity while developing a scalable decentralized medicinal services application.

Lastly, quantum computing protection is a key advantage of IOTA T-angle. It is realized that an adequately huge quantum PC could be exceptionally effective for taking care of issues that depend on experimentation to discover an answer [18]. In the Bitcoin Blockchain, one must check a normal of 268 nonce, to locate a reasonable hash that enables a new block to be created. The calculation utilized in the IOTA execution is organized to such an extent that an opportunity to discover a nonce is not substantially bigger than the time required for different assignments that are important to issue a transaction. The last part is significantly safer against quantum PC. And therefore, gives the T-angle much more protection of against an adversary with a quantum computer which is key to security demanding healthcare applications [17].

3) DAG Technologies For Healthcare Applications: As the advantages of DAG depicted above are vital for medicinal services applications, social insurance (healthcare) has turned out to be a standout amongst the most critical rising application zones of the decentralized innovation [17]. We additionally talk about the utilization cases and key advantages of embracing DAG innovation in medical domains. Some of the benefits include: enhanced healthcare record administration, enhanced protection guarantee process, and accelerated clinical research areas.

a) *Enhanced Healthcare Record Administration*: Setting up an encrypted, decentralized information store with access controls in care of the users can possibly make a more thorough record. This would empower the prescient model’s dependent on populace level healthcare information, with legitimate assent. A few surely understood organizations, such as Deloitte and Accenture, are additionally engaged with applying decentralized innovation to store medical services information and oversee healthcare records. The advantages and utilize instances of embracing DAG Tangle to enhance healthcare record administration are outlined in Table 3.

b) *Enhanced Protection Guarantee process*: Another imperative objective is to confirm the case exchanges to help healthcare financing errands. (wellbeing plan claims, for example, preauthorization installment [16]. A similar approach is Zenith certifier in [15]. The advantages and utilize instances of embracing DAG to improve insurance guarantee process are abridged in the Table 4.

Table 3. Embracing DAG tangle for Enhance Healthcare Record Administration

Key Benefit	***Health Care Use Case***
Decentralization	Enhanced consideration information sharing and examination without surrendering control: “In IOTA every participant act as a miner and validates two other transactions each time they add one to the network” [Patient] turns into the stage, owning and controlling access to their social insurance information. This evacuates all snags to patients procuring duplicates of their medicinal services records or exchanging them to another social insurance supplier [15].
Scalability	Predominant social insurance (Health insurance) information accessibility. “IOTA is exceptionally scalable and can process considerably bigger throughput as every essential actor go about as miners” [15].
Quantum computing protection	Expanded security/privacy of Healthcare records: From a security viewpoint, it is unavoidable that equipment will before long break the exemplary of cryptographic systems of IOTA Tangle. IOTA Tangle has officially arranged for the up and coming quantum headway and can oppose future progressions even with the present design [15].

Table 4. Embracing DAG to improve insurance guarantee process

Key Benefit	***Health Care Use Case***
Decentralization	Real-time case handling: IOTA makes the mining power decentralized when contrasted with other circulated decentralized techs, where incorporated control is unavoidable.
Scalability	Enhanced availability of patient information: In IOTA Tangle each member, who makes the transaction, contributes effectively dissimilar to Bitcoin where one needs to trust that the transaction will be confirmed by a digger which could take erratic time [15].
Quantum computing protection	Enhanced Privacy for Healthcare Insurance Guarantee Process: it is understood that a satisfactorily huge quantum PC could be incredibly powerful to deal with issues that rely upon experimentation to find an answer [14]. IOTA Tangle deals with this issue

c) *Accelerated clinical research areas:* The advantages and utilize instances of embracing blockchain to quicken clinical research are summarized in Table 5.

Table 5. Embracing DAG to accelerate clinical research areas

Key Benefit	*Health Care Use Case*
Decentralization	Enhanced medical information sharing: T-angle can be deployed to enhance clinical research areas, all users are considered as participants in T-angle network hence, and healthcare centers can work together with each other without relying upon some mining expert or nodes.
Scalability	IOTA T-angle system is considered to be scalable [15] hence can be used to handle Robust medical services information accessibility. The increase in number of transactions implies a stronger network and confirmation rate get better.
Quantum computing protection	Safeguarding social insurance information sharing: quantum computing protection is a key advantage of IOTA T-angle [18]. Hence, research information sharing can be handled securely.

IV. CONCLUSION AND FUTURE WORKS

A. Conclusion

We reviewed some cryptographic and decentralized algorithms and analyzed them in healthcare use cases. Symmetric and Asymmetric is a cryptography procedure utilized for securing the data while for decentralized technology, Blockchain is widely adopted. However, in reviewed cryptographic methods, users depend on a central service provider to ensure these techniques are adequately implemented. Service providers are regarded to be 'trusted but curious' in this case data are still subject to attacks. Decentralized techniques reviewed solved the centralized authorities' issues and also addressed limitations of blockchain in healthcare by implementation of DAG Tangle algorithm.

B. Future Works

Cryptography is the most known technique for ensuring security and privacy of the data by encryption. These techniques are put into use by a central authority; however, several decentralized techniques have been proposed to make user or data owners in control of their data [1] and [10]. This technique, however, has scalability issues based on blockchain formation process [14]. Future work will be that takes advantage a DAG Tangle [14] approach to design a framework for Enhanced Healthcare Insurance Guarantee Process.

REFERENCES

1. G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data", IEEE Security and Privacy Workshops, 2015.
2. S. Aljawarneh, M.B. Yassein, and W.A. Talafha, "A resource-efficient encryption algorithm for multimedia big data", Multimedia Tools and Applications, 76(21), 2015, pp. 22703–22724.
3. M. Hilbert, "Big Data for Development: A Review of Promises and Challenges Development Policy Review", 34(1), pp. 135–174, 2015.
4. R. Sugumar, "Symmetric Encryption Algorithm to Secure Outsourced Data in Public Cloud Storage", Indian Journal of Science and Technology, .vol. 8, issue. 23, 2015.
5. K. Suveetha, and T. Manju, "Ensuring Confidentiality of Cloud Data using Homomorphic Encryption", Indian Journal of Science and Technology, vol. 9, issue 8, 2016.
6. I. Sukhodolskiy, and S. Zapechnikov, "A blockchain-based access control system for cloud storage", IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, 2018.
7. T.T. Kuo, H.E. Kim, and O.M. Lucila,"Blockchain distributed ledger technologies forbiomedical and health care applications", Journal of the American Medical Informatics Association, vol. 24, issue 6, 2017.
8. J. Brogan, I. Baskaran, and N. Ramachandran, "Authenticating Health Activity Data Using Distributed Ledger Technologies", Computational and Structural Biotechnology Journal, 16, 2018, pp. 257–266.
9. S. Alshehri, S.P. Radziszowski, and R.K. Raj, "Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption", IEEE 28th International Conference on Data Engineering Workshops, 2012.
10. D. Koo, J. Hur, and H. Yoon, "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage", Computers & Electrical Engineering, vol. 39, issue 1, 2013, pp. 34–46.
11. M. Chen, Y. Qian, J. Chen, K. Hwang, S. Mao, and L. Hu, "Privacy Protection and Intrusion Avoidance for Cloudlet based Medical Data Sharing", IEEE Transactions on Cloud Computing, vol. 1, issue 1, 2016.
12. J.J. Yang, J.Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment", Future Generation Computer Systems, vol. 43-44, 2015, pp. 74–86. doi:10.1016/j.future.2014.06.004
13. S.K. Pasupuleti, S. Ramalingam, and R. Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing", Journal of Network and Computer Applications, 64, 2016, pp. 12–22.
14. Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, "Intelligent cryptography approach for secure distributed big data storage in cloud computing. Information Sciences", 387, 2017, pp. 103–115.
15. M.B. Mollah, M.A.K. Azad, A.V. Lulea, "Secure Data Sharing and Searching at the Edge of Cloud-Assisted Internet of Things", IEEE Cloud Computing, vol. 4, 2017, pp. 34-42.
16. J. Wang, M. Li, Y. He, H. Li, K. Xiao, anc C. Wang, "A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications", IEEE Access, 6, 2018, pp. 17545–17556.
17. S. Popov, "The T-angle", IOTA white paper, 2018.
18. A. Wahab, M. Barlas, and W. Mahmood, "Zenith Certifier: A Framework to Authenticate Academic Verifications Using Tangle", Journal of Software & Systems Development, 2018.
19. Panetta, R., & Cristofaro, Lorenzo, A closer look at the EU-funded My Health My Data project. Digital Health Legal, 2017. 10-11.
20. Conner Fromknecht, D.V., Sophia Yakoubov CertCoin: A NameCoin Based Decentralized Authentication System. 2014.
21. Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Computational and Structural Biotechnology Journal, 16, 267–278. doi:10.1016/j.csbj.2018.07.004.
22. Powering the Physician-Patient Relationship with HIE of One Blockchain Health IT Adrian Gropper, MD. August 7, 2016.

AUTHORS PROFILE

Tahir Yinka, Olaosebikan is a MSC candidate at Faculty of Computing and Informatics, Multimedia University. His research interests include security and privacy in healthcare domain, Big data and decentralized networks.

Su-Cheng Haw is Associate Professor at Faculty of Computing and Informatics, Multimedia University, where she leads several funded research on the XML databases. Her research interests include XML databases, query optimization, data modeling, semantic web, ontology, data management, and data warehousing. She has published more than 120 articles in reputable journals and conferences.

Gaik-Yee Chan is a Senior Lecturer at Faculty of Computing and Informatics, Multimedia University. Her expertise is mainly in the areas of information security, data mining and cloud computing. She had been project leaders and members for several ministry of higher education funded research and member in an industry funded research. She has many publications in reputable journals and conferences as well.