VERIFICATION OF MEDICAL TRANSCRIPT WITH BLOCKCHAIN BASED ON PROOF OF AUTHORITY (POA) CONCEPT

Ratchapon Pockathum[1] and Adisorn Leelasantitham [1,*]
[1] Technology of Information System Management, Faculty of Engineering, Mahidol University, Thailand

ABSTRACT

Since the problem of vulnerability of the system in checking important documents has unlawful acquisition occurred for a long ago. This research presents the implementation of a decentralized document verification system. It is created mainly with Ethereum Blockchain technology, so that relevant parties can check the accuracy of applicant documents directly. The scope is focused on the document verification request process and after implementation on a test network, the result is Proof of Authority consensus is faster than the Proof of Work. Overall the system is faster, reliable, and secure. The suggestion of this study is to improve more features related to the requirement in the future.

Keywords: Ethereum, Blockchain, Proof of Authority.

1. INTRODUCTION

Every year some graduates will be obtained a degree from the university and almost everyone used this degree to represent what they have learned. Enter the world of work and further study. Figure 1 explains the current situation when we want to work or study. It has to use those educational documents [1] to apply. In the field of Medical, there are differences from a normal career. They must have Licensed to Practice Medicine follow from the law and has expiry date [2].

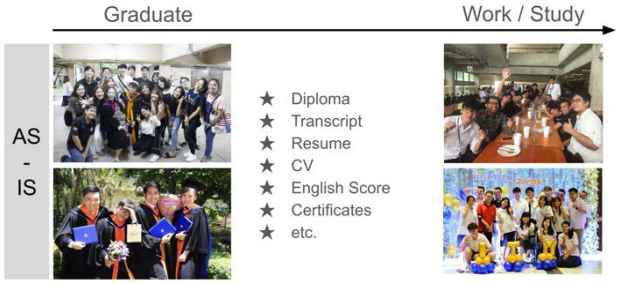


Figure 1. Essential documents to apply to work or study

Manuscript received on April 15, 2020; revised on July 7, 2020.
[1,*]Corresponding author Email: adisorn.lee@mahidol.ac.th Technology of Information System Management, Faculty of Engineering, Mahidol University, Thailand.

On the other hand, the problem of unlawful acquisition of cheating is something that has come for a long time [3]. There are illegal shortcuts to find work or increase salaries by using the vulnerability of the system in checking important documents of the universities, government offices, private or public companies. However, the current process of verifying the document is rather difficult, and the lack of an efficient validation system.

Since there is a case of fake nurse that works for 11 years and it damages patients, hospital and affects to Thailand nursing council and the university that fake nurse uses fake degree and fake nurse license [4], as shown in Figure 2, There are various ways to solve the problem such as a centralized system and decentralized system. This research is aimed to Implement a decentralized document verification system to avoid fake documents using blockchain Proof of Authority network. Previous medical work research applies blockchain and the result is can improve the efficiency of the system with more security and decrease process time.

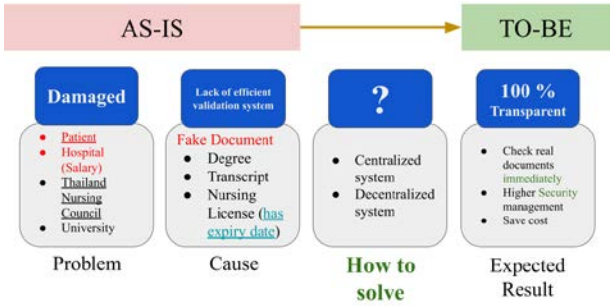


Figure 2. Problems, solutions, and expected results

2. LITERATURE REVIEW

This section, consist of three basic concepts that relates to the research: glossary, consensus comparison matrix and related work.

2.1 Glossary

A. Centralized network: Communication between users and trusted parties. All users have to go through a single centralized source. If the central is attacked or down, the entire system and users cannot communicate with each other [5].

The current situation of document verification. It spends time for many days, as shown in Figure 3, In the case of the organization manual verification, there is the process of writing a request letter and send an email to the centralized organization, then the centralized organization verify the document and sends the result to the company [6]. If the central intermediary is down or attacked, the entire network stops working (Single-point-of-failure) [7].

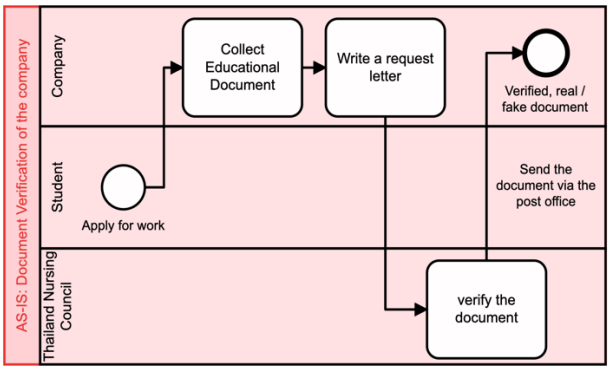


Figure 3. Document verification of the company

B. Decentralized network: Multiple trusted parties as a centralized hub for a subsection of users. Some users are using a centralized hub. If the centralized hub is attacked or down, that centralized hub will not communicate with those users [5].
C. Distributed network: A network configuration where every user can communicate each other without going through a centralized point because can communicate with the multiple pathways, the loss of any user will not prevent communication. This is also known as a peer-to-peer network [5].
D. Blockchain: Distributed digital ledgers that have a cryptographically in each transaction grouped into blocks. Each block cryptographically linked to the previous one [5]. The data in previous block cannot be modified.
E. Ethereum: The open source decentralized applications platform uses Smart contracts to control the transaction protocol. The term smart contract defined by Nick Szabo in 1994.
F. IPFS: The interplanetary File System is a distributed system for storing and accessing files, websites, applications, and data.

2.2 Consensus comparison

A. Proof of Work Consensus Model

Proof of Work (PoW) is the original consensus algorithm in a Blockchain network. A user publishes the next block by being the first to solve a computationally intensive puzzle called “miner” and a process is called “mining”. The solution to this puzzle is the “proof” they have performed work. This enables all other full nodes to easily validate next blocks and will reject block that did not satisfy the puzzle [5].

B. Proof of Authority Consensus Model

The proof of authority (PoA) consensus relies on the trust parties to publishing nodes. Publishing nodes must have their identities proven and verifiable within the blockchain network. The idea is the publishing node is staking reputation to publish new blocks. Blockchain network users directly affect a publishing node’s reputation that can be good or bad based on the publishing node’s behavior. This algorithm only applies to blockchain networks with high levels of trust [5].

2.3 Related work

Back on October 31, 2008, Satoshi Nakamoto created a cryptocurrency or bitcoin that could send money between them without going through an intermediary and creating ideas for a blockchain [8]. And people who started to think that aside from sending money matters can be used in various fields as well. One person is Vitalik Buterin, founder of Ethereum His paper was released in 2013 [9] and started his project in 2015. Ethereum is a cryptocurrency and opensource software that can be used to build advanced applications. In his paper, he mentioned the smart contract, which is part of the code. That is the main part of Ethereum. Nowadays, it is increasingly used in other areas such as Electricity Utility Systems that they use to decrease the costs to consumers, prosumers and SMEs obtained from the use of blockchain technology are possibly lower than trusted third-party in the future [10], medicine, education (sharing certificate documents [11], higher education credits [15]), donations, etc. Most of the work will use the Ethereum Blockchain to develop and use the Proof of Work Consensus [7]. The consensus is the rules set forth from the beginning and everyone in the system will strictly abide by this rule. In the world of Blockchain, there are many ways to confirm and adhere to the common agreement of the whole network [5]. The most commonly used is Proof of Work because it is the first concept from cryptocurrency [8]. And is a consensus that the Ethereum can develop therefore commonly used in research Aside from Proof of Work, there are Proof of Stake and Proof of Authority. Which we will use Proof of Authority because the speed.

As shown in Figure 4, it is tested via a simulated network. There will be 3 PoA test networks, including Ropsten Kovan Rinkeby and Sokol. Each test network will have different support [12]. Other researches also apply blockchain to other systems. For example, a combination of blockchain and central database [13], a combination with file storage using IPFS [13][14][16]. There is a ranking blockchain ranking in 2019 made by The Center for Information and Industry Development (CCID), which is an agency under the Chinese government. The Ethereum is ranked number 2 [17] shown in Table1. Therefore, when looking at the problems and solutions to a wide variety of problems. The purpose of this research is to create a document checking system using a blockchain based on Proof of Authority concept.

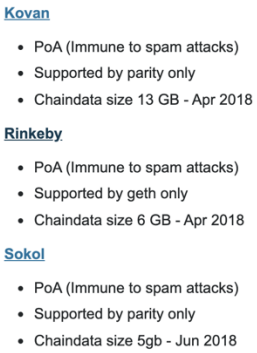


Figure 4. Proof of Authority Ethereum test network

Table1: CCID's Global Public Blockchain Technology Assesment Index (15)

Pub-Blockchain	Sub-Index			Total Index	Ranking
	Basic-tech	Applicability	Creativity		
EOS	104.6	21.6	25.2	151.4	1
Ethereum	75.7	30.6	31.7	138.0	2
TRON	94.2	25.4	18.2	137.8	3
NULS	76.7	18.8	18.1	113.6	4
Lisk	65.9	15.2	29.4	110.5	5
NEO	69.6	26.0	11.5	107.1	6
STEEM	85.6	10.1	10.5	106.2	7
BitShares	82.6	15.0	7.8	105.5	8
Bitcoin	42.6	18.5	42.9	103.9	9
XLM	70.1	21.5	10.9	102.5	10

3. METHODOLOGY

This section consists of the proposed system, scope of system, data dictionary, solidity contract structure, implement environments and tools, and application prototype / demonstration.

3.1 The proposed documents verification system

The proposed solution is to implement the blockchain document verification system to decrease time and cost and increase the security of the system. Figure 5 explains the process of proposed solution that the trusted organization (Thailand Nursing and Midwifery Council) create and store the essential documents for nurse in digital format such as text, convert a file to a hash value, and hash address. The essential document in paper form will have a hash value. It can be in various term example is a QR code that keeps the hash value of nurse license. After the nurse applies for work at the company. The company can verify from the nurse's document by a search for that hash value and can see more updated detail by pay some amount of cryptocurrency value to view the information.

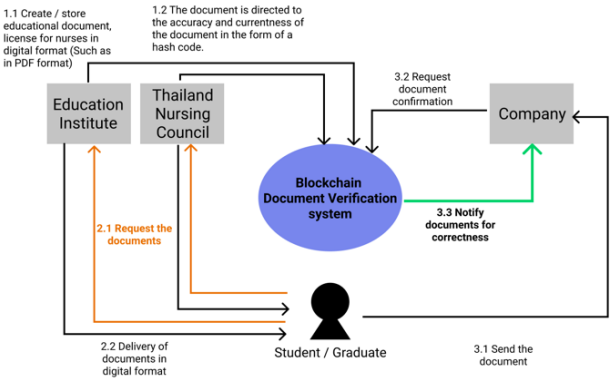


Figure 5. Blockchain Document Verification System

3.2 Scope of system

Figure 6 shows the scope of the system focuses on the verification process. The company can request the document through the system and have to pay some amount of value in terms of Wei units. The verification system allows companies to view the current information of the requested.

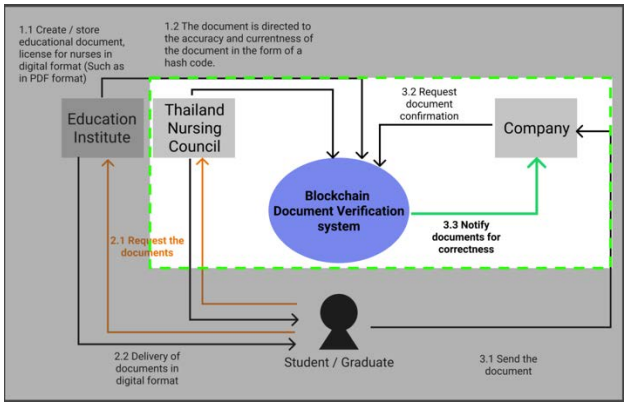


Figure 6. Scope of Document Verification System

3.3 Data Dictionary of Nursing License

The Nursing License included the license number, Renewed number (In case of renewal), First name, Surname, Position step, Date of Issue (Day, Month, Year), Expiry Date (Day, Month, Year), Secretary-General Signature of the Nursing Council, and President Signature of the Nursing Council.

3.4 Solidity Contract Structure

Figure 7 shows the relation to the example of a contract structure that will use to implement the system consist of variables of manager that will collect the address of the person who is managing this License, payment Per Request is set by the manager and the companies have to pay as that setting, companies variable is List of address for every person who has pay for the document request. Document Detail is a list of document detail struct that the

manager has created an example of struct store the data of license Number, IPFS Hash, name, surname, public ID, and more depend on additional needs. Functions consist of a Constructor function called Nursing License that sets the payment per request, and the address of the manager. Create Request function called when a company wants to request the document by requiring a payment amount that equates to the manager set up.

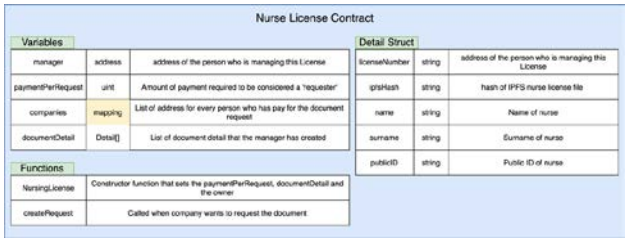


Figure 7. Nurse License Contract

3.5 Flowchart of Blockchain

Figure 8 shows the flowchart explaining the overall process that creates a decentralized application. The first step is creating and test a smart contract on the remix. After that, setup Infrastructure on a local computer includes build compiler and deploy file. Before going to deploy the real one, it is more important to test the contract on the local computer. After the backend part, the next step is designing a mockup and create the frontend part consist of React and Next.js. After get all pages to follow from mockup when want creates something. The metamask page will pop up to make a confirmation of that function in a smart contract. If the input is passed as a condition in the contract is written. A transaction will be created and display information.

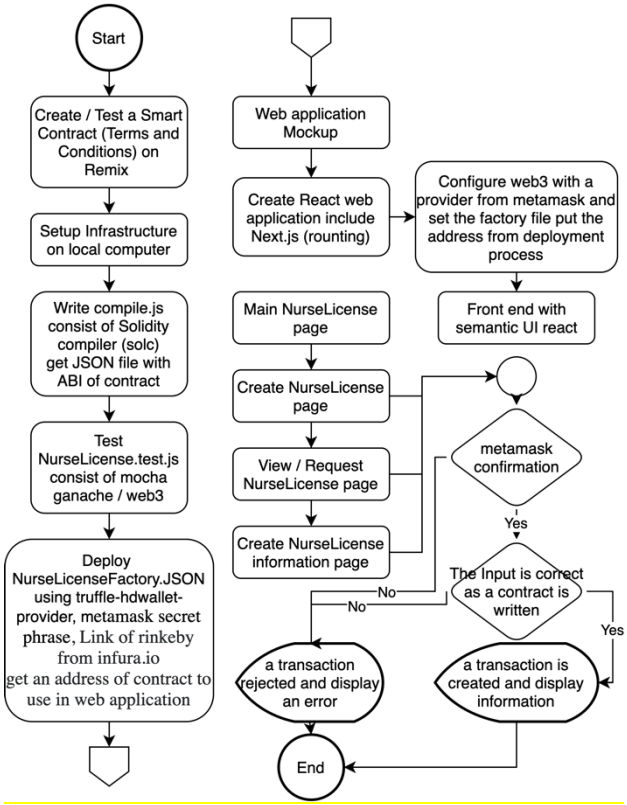


Figure 8. Flowchart of the system

3.6 Implementation environments and tools

The system is developed on Mac Operation System, Visual Studio Code, React JS, Next JS. Start implement on remix.ethereum.org to do a test with solidity code and run on the Ethereum environment, Brave or Chrome Browser, Nodejs, Metamask, ganache, Infura, web3 JS.

3.7 Application Prototype / Demonstration

The prototype was designed and divided the page into 4 pages. There are the main page, set payment per request page, overview page, and create document information page. The prototype design is shown as the following. As shown in Figure 9, the main page consists of a list of nurse license address, a view of button to link to overview page, and a created button to link to set payment per request page.

Figure 9. Main page

Figure 10 shows the page of the user can fill the value (Wei) to set the payment that companies have to pay to view the information and when press create button. It will link back to main page with addition nurse license address.

Figure 10. Set payment per request page

After the press, Figure 11 shows a button view of the selected nurse license address block on the main page will link to the overview page that contains the list of information. There are address of manager who creates the nurse license by setting the payment from the previous page, current active address that signed in Metamask, amount of payment that companies have to pay for request, number of requests, the balance of this nurse license address, and list of information table that show the create

history and will highlight on current information. Figure 12 shows the page of the manager can fill the essential information that consists of nurse license data dictionary.

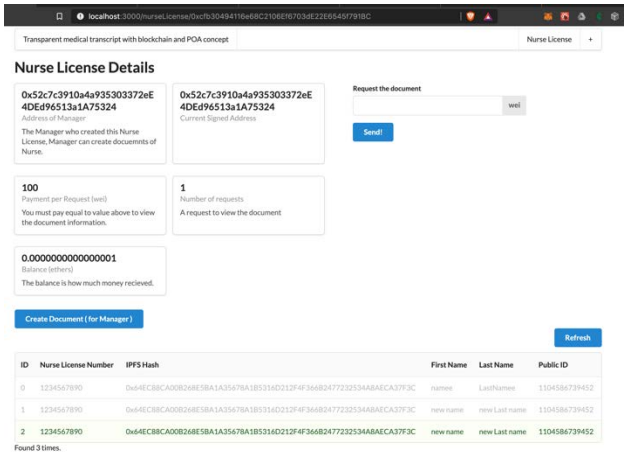


Figure 11. Overview page

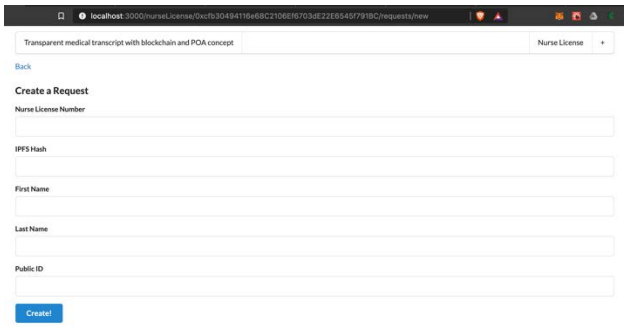


Figure 12. Document information creation page

4. EXPERIMENTAL RESULTS AND DISCUSSION

This section explains the computer specification, performance of the system and Discussion.

4.1. Computer Specification

The computer spec that use to implement and run the results is Mac OS Catalina 1.6 GHz Dual-Core Intel Core i5.

4.2. Test Network

The Ethereum test network that uses is the Rinkeby network because of the implementation of Proof of Authority consensus and go-Ethereum development [12].

4.3. Experimental results

There are compare the speed between the current process and document verification system with blockchain based on Proof of Authority consensus. The performance of the current process and Proof of Authority consensus is shown in Table 2.

Table2: The speed performance of Proof of Authority consensus and current process

Type of consensus	Average Transaction Speed
Proof of Authority (PoA)	15 seconds
Proof of Work (PoW)	30 seconds

4.4. Discussion

The performance of Proof of Authority consensus is faster than the Proof of Work. Due to the different systems and processes as mention in figure 3 in Section 2.1A. The use of Proof of Authority is suitable for use in a reliable company. The result is related to the literature review that it spends not much time to run a transaction and can solve the problem of research that can check all documents history and ensure that the previous data cannot edit.

5. CONCLUSION AND FUTURE WORK

This research implements on the Ethereum blockchain and Proof of Authority network, when compared with the current system and process. The blockchain system faster than the current system, so it improves the performance of the thrust organization. The ways to improve can change the process of creating the document by a nurse and improve the more complicated function of the system. Overall the system is faster, reliable, and secure. The suggestion of this study can be comparative between Proof of Work and Proof of Authority consensus, can do in a private blockchain network, and improve more features related to the requirement in the future.

REFERENCES

[1] Jones, Jane Redfern. (2006). *First impressions count: job application letters are your opportunity to sell yourself and your skills*. Nursing Standard, vol. 20, no. 25, p. 72. Gale OneFile: Health and Medicine, Accessed 29 May 2020.

[2] Thailand Nursing and Midwifery Council, Renew Nurse License, Available from: https://www.tnmc.or.th/news/43 [Retrieved 2020]

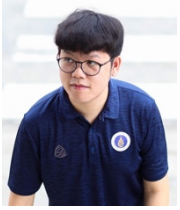
[3] Transparency International. (2013). *Global Corruption Report: Education*, SICE, New York.

[4] Workpoint Today, Studied for real, but didn't graduate, disguised as a nurse for 11 years, Available from: https://workpointtoday.com/male-nurse-1[Retrieved 28 August 2019]

[5] D. Yaga, P. Mell, N. Roby, T. Keisoku. (2018). *Blockchain Technology Overview*, *NISTIR8202*.

[6] Thailand Nursing and Midwifery Council, "Requesting to check the professional license status",

Available from: https://www.tnmc.or.th/news/50 [Retrieved 2020]
[7] Kuo TT, Kim HE, Ohno-Machado L. (2017). *Blockchain distributed ledger technologies for biomedical and health care applications*. J Am Med Inform Assoc. , 24(6), 1211-1220. doi:10.1093/jamia/ocx068
[8] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, Available from: https://bitcoin.org/bitcoin.pdf
[9] V. Buterin. (2013). Ethereum: The Ultimate Smart Contract and Decentralized Application Platform, Available from : https://web.archive.org/web/20131228111141/http://vbuterin.com/ethereum.html
[10] A. Leelasantitham. (2020). *A Business Model Guideline of Electricity Utility Systems Based on Blockchain Technology in Thailand: A Case Study of Consumers, Prosumers and SMEs*, Wireless Personal Communications, February 13, 2020, Available from: https://doi.org/10.1007/s11277-020-07202-8.
[11] S. Kolvenbach, R. Ruland, W. Gräther, W. Prinz. (2018). *Blockchain 4 Education*, In: Proceedings of 16th European Conference on Computer-Supported Cooperative Work -Demos and Posters, Reports of the European Society for Socially Embedded Technologies, ISSN 2510-2591, DOI:10.18420/ecscw2018_p7
[12] Comparison of the different TestNets, Available from:https://ethereum.stackexchange.com/questions/27048/comparison-of-the-different-testnets [Retrieved 2017]
[13] H. L. Pham, T. H. Tran, Y. Nakashima. (2019). *Practical Anti-Counterfeit Medicine Management System Based on Blockchain Technology*, 4th Technology Innovation Management and Engineering Science International Conference (TIMES-iCON), Bangkok, Thailand, pp. 1-5,doi:10.1109/TIMES-iCON47539.2019.9024674.
[14] O. Shigenori, W. Hiroki, I. Tatsuro, F. Shigeru, N. Atsushi, K. Jay. (2019). *Token-Based Sharing Control for IPFS*, 361-367. 10.1109/Blockchain.2019.00056.
[15] Marko H., Kristjan K., Marjan H., Aida K. (2018). *EduCTX: A blockchain-based higher education credit platform.*
[16] N. Muqaddas,A. Fahad, K. Rabiya, J. Nadeem, Q. Ali, A. Muhammad, S. Muhammad. (2019). *A Secure Data Sharing Platform using Blockchain and IPFS*, doi: 10.3390/su11247054.
[17] J.Siribunchawan, What is and EOS coin? Why do many people think that it will finally beat Ethereum?, Available from: https://siamblockchain.com/2018/12/04/what-is-eos/ [Retrieved 2018]



Ratchapon Pockathum was born in Bangkok, Thailand in 1994. He received the B.Sci. in Information Communication and Technology (international program) from the Mahidol University, Nakhonpathom, Thailand in 2017 and Studying M.Sci. in Information Technology Management at the same university. Currently, he is a computer technical officer at Faculty of Graduate Studies, Mahidol University. His interests include blockchain.

Adisorn Leelasantitham received the B.Eng. degree in Electronics and Telecommunications and the M.Eng. degree in Electrical Engineering from King Mongkut's University of Technology Thonburi (KMUTT), Thailand, in 1997 and 1999, respectively. He received his Ph.D. degree in Electrical Engineering from Sirindhorn International Institute of Technology (SIIT), Thammasat University, Thailand, in 2005. He is currently the Associate Professor in Technology of Information Sys- tem Management Program, Faculty of Engineering, Mahidol University, Thailand. His research interests include applications of blockchain technology and cryptocurrency e.g. electricity trading platform etc., conceptual models for IT managements, image processing, AI, neural networks, machine learning, IoT platforms, data analytics, chaos systems and healthcare IT. He is a member of the IEEE.