Journal of Advanced Research in Technology and Management Sciences
Volume: 05 Issue: 05 ISSN: 2582-3078 May 2023
Available online at: http://www.jartms.org

CHAINGUARD: A BLOCKCHAIN-BASED SOLUTION FOR SECURING E-HEALTH RECORDS

Hemanth Reddy.G[1], Dr. N. Praveena[2], Harsha Vardhan.V[3], Charan Kumar Reddy.K[4], Gopinath Reddy.M[5]

[1] *Assistant Professor Department of Computer Science and Technology, Madanapalle Institute of Technology & Science, Madanapalle.*

[2,3,4,5] *UG Student Department of Computer Science and Technology, Madanapalle Institute of Technology & Science, Madanapalle.* **Email:** [1]*hemanthineuron@gmail.com,* [2]*praveenan@mits.ac.in,* [3]*harshavardhan95336@gmail.com,* [4]*charanreddy0811@gmail.com,* [5]*gopir7213@gmail.com*,

***Abstract*— In recent years, there has been a significant shift in how Electronic Health Records (EHRs) are stored, with a new model that offers low operational costs, high flexibility, and availability. However, this shift also raises concerns about data privacy and network security for e-health systems, particularly when it comes to sharing EHRs among mobile users. Addressing this challenge requires a reliable approach that can ensure high levels of security while facilitating the sharing of EHRs. To that end, we propose a novel framework that combines blockchain and the decentralized interplanetary file system (IPFS), with a focus on developing a trustworthy access control mechanism that uses smart contracts to enable secure EHRs sharing among different patients and medical providers. The present project is focused on tackling security and scalability issues within the healthcare industry through the utilization of blockchain technology and storing purpose using IPFS. By adopting a decentralized and trustworthy approach to electronic health record sharing, data access can be streamlined for both patients and healthcare providers across multiple organizations. To ensure secure and efficient EHRs sharing, our proposed system employs a user access control framework that manages data access from various network entities. This framework effectively prevents unauthorized access to EHR resources, while allowing authorized entities to retrieve data quickly and easily. With the implementation of this control mechanism, we aim to establish a trusted platform for sharing EHRs, where only authorized users have access to modify and view data. The system is achieved to boost data security, integrity, and maintain trust between users and technology.**

***Keywords*—Electronic Health Record(EHR), Interplanetary file system (IPFS), Blockchain Technology**

I. INTRODUCTION

Nowadays with rapid growth in Technology in every field, there are several drawbacks like Security issues, Scalability issues. With this project, we are addressing one such issue in the Health Care field. In the present day, we can see there is rapid growth in Blockchain Technology which helps to address various issues. Blockchain is a decentralized and Trustworthy technology that provides great results in e- health care of the patient and it will be helpful in ease of data access even among one or more health care Organizations, it will make the work easier for the patient as well as doctors. Blockchain technology has been increasingly explored as a potential tool in the healthcare industry sector will give better results. As the name suggests blockchain consists of Several blocks are connected in the form of a chain. The blocks will be useful to store the large amount of Data Securely.

These blocks are secured with a Secure hash Algorithm in which every block generates a unique hash code based on the provided input to the block. The Blockchain also Consists of a feature called Ledger in which every person in that blockchain will get to know everything about the data,and what's happening with that data if any person tries to modify the data in the blockchain then everybody will get to know that some data modification has happened in the blockchain.

By using this blockchain is efficient in providing security for the stored data. Along with blockchain mobile cloud computing is an emerging technology that has witnessed significant changes in the healthcare industry. A patient can get their health data on their smartphones through apps and detailed reports. The cloud will serve the user with whatever he needs but at the same time, there is a threat to the patient or user's data. But the blockchain comes into the picture when the users and healthcare industries mainly started focusing on the security and Integrity of Data. Unauthorized access to data is the main problem with the previous technologies.

The traditional methods are not so efficient in meeting all these requirements so nowadays we can transition from traditional methods to the Blockchain which is a decentralized model in which the data is decentralized among several blocks in the sense that the authority of data will be distributed among several people. In each block, it Consists of relevant information, Hash Code, and previous block hash value, the first block does not contain any previous block value, first block is called a genesis block. With the help of Blockchain, it is easy to track the data and it also keeps the data Unique it is quite difficult to get stolen this is the reason it is the most secure technology in terms of data storage. If an attacker tries to modify information, the hash value automatically changes in every block. The Blockchain has also some set of rules one among them is the consensus rule, which states the change in the blockchain needs to be accepted by the majority of people in the blockchain . Blockchain also consists of smart contracts which are made using some programming languages like Solidity. In the end, blockchain will overcome all the drawbacks that are there in previous or traditional technologies and increase the security and integrity of data and will maintain trust between users and Technology. Our proposed system is built on a user access control framework designed to manage data access from network entities. With efficient access control mechanisms in place, illegal access to EHRs resources can be effectively restricted while ensuring prompt data retrieval for authorized entities.

II. RELATED WORK

A.BLOCKCHAIN TECHNOLOGY FOR EHR

Blockchain technology enables a distributed, decentralized network environment without the need for a central authority. Using cryptographic standards ensures the security and reliability of transactions. Due to the increasing usage of digital forms of currency, blockchain innovation has recently become fashionable, popular, and pervasive in many sectors. The need for a more patientcentric approach to healthcare systems, increased system interoperability, and increased precision of Electronic Healthcare Records (EHRs) make healthcare one industry where blockchain innovation has enormous promise. This led to a poll being conducted [5], which revealed growing interested in blockchain technology in the healthcare industry. Research indicates that the adoption of blockchain technology in the healthcare sector is expanding, primarily focusing on information sharing, health data management, and access regulation, with limited usage in other scenarios is growing and that it is mostly used for information exchange, managing health data, and access control. Other situations are quite rare.

B.RESEARCH

He.Kim's [1] study focuses on the blockchain distributed ledger technology's scalability constraints, which can limit the number of transactions allowed.

Yanzhung's [2] patient-centric health info exchange framework, although secure, requires a separate setup at each healthcare facility, which can lead to scalability issues.

J. Indumathi's[3] blockchain-based IOT for unlimited healthcare services faces challenges due to the consensus algorithm's improper functioning with IOMT devices.

Guangjun wu's[4] privacy preferred medical record exchanging and sharing a blockchain-based health system addresses transaction latency and is individual-centric. However, it consumes time due to its dynamic access control framework with LDP.

Ayesha Shahnaz's[5] study on using blockchain for healthcare records focuses on data transparency, security, and privacy but faces challenges related to storage capacity.

Rahul Ganpatro sonkamble's[6] survey of interoperability in EHRM proposes a blockchain-based framework for privacy for user data but faces challenges related to access cost.

Rui P. Pinto's[7] system for the promotion of traceability and ownership of health data using blockchain focuses on enhanced security and privacy of patient data but faces scalability constraints.

Shufen Niu's[8]” EHR sharing scheme with searchable attribute-based encryption addresses data correctness and security but consumes a lot of time.

Zhen Pang [9]proposed a model for sharing Electronic Health Records (EHRs) using Blockchain technology and the Checkable state PBFT consensus algorithm, but the scalability constraints still need to be further addressed.

III. PROPOSED WORK

The proposed blockchain system would have various users, including patients, doctors, and administrative staff. Their main responsibility would be to interact with the system and perform basic tasks such as creating, reading, updating, and deleting medical records. To access the system's functionalities, users would require a DApp browser, which would contain the graphical user interface (GUI) of the proposed system framework. The GUI would provide all the necessary functions that a particular user would require. Depending on their assigned role, users would be able to use the GUI to interact with the blockchain layer of the system.

A. Algorithms

There are several algorithms used in blockchain for securing electronic healthcare records (EHR).

Hashing: Hashing is a cryptographic method that converts data or a message into a string of characters of a predetermined length. This hash value is specific to the input data, therefore any modifications to the data will produce a new hash value. To generate a tamper-evident and tamper-resistant record of EHR transactions, blockchain employs hashing. Data integrity and authenticity are protected using hashing in conjunction with other cryptographic techniques like digital signatures.

Asymmetric cryptography is another name for public key cryptography, which encrypts and decrypts data using a set of two keys (public and private). Digital signatures that are connected to transactions in the EHR system via blockchain are produced using public key cryptography. These electronic signatures are employed.

Proof of Work: A consensus mechanism called Proof of Work (PoW) is used in blockchain to authenticate transactions and add new blocks to the network. To confirm a transaction or build a new block in PoW, users must solve a challenging mathematical puzzle. The EHR system is safe and resistant to assaults because of this algorithm.

Proof of Stake: Another consensus technique used in the blockchain is Proof of Stake (PoS). In contrast to PoW, players in PoS are not required to solve challenging mathematical puzzles. To validate transactions and add new blocks, PoS players must stake a particular amount of cryptocurrency. This algorithm, which prioritizes energy efficiency in blockchain systems, is more energy-efficient than PoW.

Blockchain technology uses **Merkle trees,** a type of data structure, to store and validate vast volumes of data. Each leaf node in a Merkle tree represents a data block, while each non-leaf node represents the hash value of its offspring nodes. Without needing every blockchain node to authenticate every transaction, merge trees are used to efficiently check the validity and integrity of data on the blockchain.'

B.Generic Algorithm Proposed Framework

//Assign Roles:

```
function defineRoles (string memory newRole, address newAccount) public {

// Adding new role and account to the roles mapping

roles[newRole] = newAccount;

}
```

//Adding Data:

```
function addPatientRecord (string memory patientId, string memory name, string memory data) public {
```

```
// Verify that the sender is a doctor

Require (msg. sender == roles["doctor"], "Only doctors can add patient records.");

// Add data to particular patient's record

patients[patientId][name] = data;

}

//Retrieve Data:

function viewPatientRecord (string memory patientId) public view returns (string memory) {

// Verify that the sender is a doctor or the patient

Require (msg. sender == roles["doctor"] || msg. sender == roles["patient"], "Only doctors and patients can view patient records.");

// Retrieve data from specified patient

return patients [patientId] [msg. sender == roles["doctor"] "doctor_view" : "patient_view"];

}

// Update Data:

function update patient record (string memory patientId, string memory name, string memory data) public returns (bool) {

// Verify that the sender is a doctor

Require (msg. sender == roles["doctor"], "Only doctors can update patient records.");

// Verify that the patient id and name match

If (keccak256(bytes(patient)) == keccak256(bytes(name))) {

// Update data to particular patient's record

patients[patientId][name] = data;

return true;

} else {

return false;

}

}
```

// Delete Data:

```
function deletePatientRecord (string memory patientId) public returns (bool) {

// Verify that the sender is a doctor

Require (msg. sender == roles["doctor"], "Only doctors  can delete patient records.");

// Delete a particular patient's record

delete patients[patientId];

return true;

}
```

Step1: Define a function called "defineRoles" that takes a new role and account as parameters and adds them to a roles mapping.

Step2: Define a function called "addPatientRecord" that takes patientId, name, and data as parameters.

Step3:Verify that the sender is a doctor using the "Require" function.

Step4:Add the data to the specified patient's record.

Step5:Define a function called "viewPatientRecord" that takes patientId as a parameter and returns the data associated with the patient.

Step6:Verify that the sender is a doctor or the patient using the "Require" function.

Step7:Retrieve the data from the specified patient's record.

Step8:Define a function called "updatePatientRecord" that takes patientId, name, and data as parameters.

Step9:Verify that the sender is a doctor using the "Require" function.

Step10:Verify that the patient id and name match.

Step11:Update the data associated with the specified patient's record.

Step12:Define a function called "deletePatientRecord" that takes patientId as a parameter.

Step13:Verify that the sender is a doctor using the "Require" function.

Step14:Delete the specified patient's record.

Step15:Return true if the operation is successful, otherwise return false

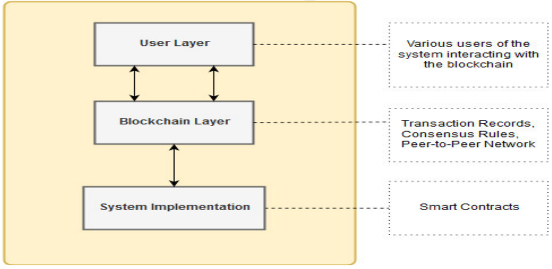

User Layer
Various users of the system interacting with the blockchain
Blockchain Layer
Transaction Records, Consensus Rules, Peer-to-Peer Network
System Implementation
Smart Contracts

Fig1:System design for Proposed Framework

This system is designed to serve a variety of users, including patients, doctors, and administrative staff. Their main task will be to interact with the system and perform basic functions such as creating, reading, updating, and deleting medical records. These users will access the system's functionality through a browser, which we refer to as a DApp browser, as it contains the graphical user interface (GUI) of the DApp, or our proposed system framework. The GUI includes all the functions that a particular user can access. Depending on their assigned role, users can use this GUI to interact with the other layer of the system, namely the blockchain layer.

IV. Performance Analysis

In order to evaluate the effectiveness of the system, several metrics have been considered. These include the execution time, latency, and throughput.

Execution time is measured as the time duration (in seconds) between the confirmation of a transaction and its execution on the blockchain network.

Throughput, on the other hand, refers to the amount of data that can be transferred between two locations within a given time period.

Finally, latency is defined as the delay that occurs when a system component is waiting for another component to respond to an action. In terms of time , latency is calculated as the difference between the deployment and completion times of a transaction.

A.Scalability

In the case of blockchain technology, scalability is a crucial issue that requires a permanent solution. As the amount of data stored on the blockchain increases, the proposed system addresses scalability by using an off-chain storage mechanism. Our proposed system stores patient data on the blockchain, but with only essential information and an IPFS hash to act as an off-chain scaling solution. This approach reduces the amount of patient medical records stored on the blockchain, leading to faster transaction processing times. Moreover, IPFS leverages a cryptographic hash that is stored in a decentralized manner using a peer-to-peer network, ensuring that scalability is not compromised

B.Integrity

The trustworthiness of a system's integrity relies on the ability to store information in reliable manner. A blockchain-based system guarantees this feature, as it prevents unauthorized changes to the stored information and limits access to only authorized parties such as doctors and patients. Access rules are in place to protect private medical records, ensuring they remain secure and inaccessible to third parties. Additionally, using IPFS for record storage further enhances the security of patient medical records.

C.Access Control

The framework employs a Role-based access mechanism that assigns roles to every entity in the system, ensuring that only authorized users can access it. Unauthorized third parties are denied access. The system's security is further strengthened by the use of blockchain technology, which is inherently secure and utilizes various protocols and mechanisms to prevent intrusions. By limiting access to users with defined roles, our system not only safeguards patient records but also ensures access control of associated entities. This approach guarantees that patient data remains secure and only accessible to authorized users of the system.

*D.*Content Addressable Storage

Content-addressable storage is a storage mechanism utilized by IPFS to store data off-chain. In this approach, a hash data is generated, the hash is stored on blockchain, while the data is stored on IPFS. The hash serves as a reference to the stored data and can be accessed by authorized parties such as doctors and patients. The use of content-addressable storage ensures the security of the stored data, as the generated hash is cryptographically secure. This approach is commonly used in blockchain-based systems to maintain the integrity and security of sensitive information, and it is an effective mechanism to ensure the protection of patient records.

E.Throughput

Throughput refers to the successful message delivery rate over a communication channel. In the context of blockchain, it indicates the number of transactions processed per unit of time, and serves as a critical metric for evaluating the overall performance and scalability of a blockchain network.

Throughput = Number of Transactions / Time Taken

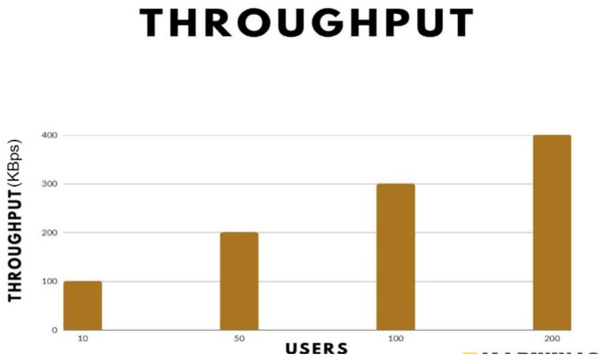


Fig2.Throughput for Proposed Framework

The smart contract of the proposed framework is outlined, which includes various functions. To evaluate the system's performance, we utilized JMeter to simulate the usage of the system by 10 to 200 users over a period of 10 to 35. The throughput was measured in KB/sec, and the performance of the system was analyzed based on these simulations. The outcome of the trial demonstrated a proportional rise in the throughput of the system with an increase in both the number of users and requests.

The efficiency of the proposed framework is emphasized by the observed linear increase in throughput and its ability to handle a higher volume of users and requests without experiencing a decline in performance. Figure 2 provides a visualization of the observed throughput

F. Average Latency

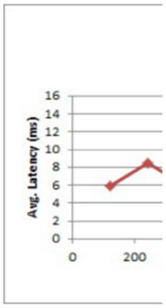


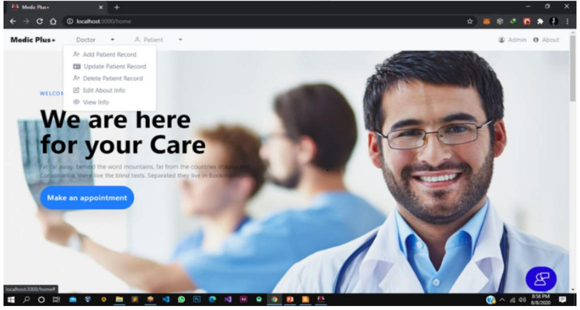
Fig3: Average Latency

	[5]	[6]	[7]	Our System
Blockchain Based Technology	Y	Y	Y	Y
Scalability	Y	Y	N	Y
Content-Addressable Storage	N	N	N	Y
Integrity	Y	Y	Y	Y
Access Control	Y	N	Y	Y

Latency, as previously stated, is the time difference between when one system component submits a request and when another system component generates a response. Latency is defined as the difference between these two activities. Using JMeter

The figure shows an overview of the system's average latency as well as the throughput of the suggested framework. In this experiment, the longest measured delay is 14ms.We also investigated the suggested framework's performance by examining transaction size and cost. Before deciding on the transaction size, we analyse the transaction payload the next sections go over this examination in detail.

G. Performance Evaluation



Far far away, behind the word mountains, far from the countries Vokalia and Consonantia, there live the blind texts. Separated they live in Bookmarksgrove

Fig4.User Interface

The above figure represents User Interface there are mainly three modules Admin, Doctor and Patient. The role of Admin is Adding Doctors to the Network, and the role of doctor is consulting to the patients, adding medical records, updating medical records and also deleting the medical records and the role of patient is make an appointments with the doctor and can also view their medical records.

CONCLUSION

This project delves into the potential of blockchain technology in addressing issues faced by the healthcare sector and electronic health record systems. Our proposed framework incorporates secure record storage and precise access rules, enhancing user experience and comprehension. We also address the challenge of data storage by utilizing the IPFS off-chain storage mechanism, and the role-based access ensures that only trusted and relevant individuals have access to medical records, thereby mitigating the issue of information asymmetry.

REFERENCES

[1] H. E. Kim, Kuo, T.T., and Ohno-Machado, L. "Blockchain distributed ledger technologies for biomedical and health care applications." Journal of the American Medical Informatics Association, vol. 24, no. 6, pp. 1211-1220, 2017.

[2] X. Yuan, S. Lu, W. Lu, and D. Chen, "A Patient-Centric Health Information Exchange Framework Using Blockchain Technology," IEEE Access, vol. 7, pp. 49026-49037, 2019.

[3] J. Indumathi, Achyut Shankar, Muhammad Rukunuddin Ghalib, J. Gitanjali, Qiaozhi Hua, Zheng Wen, and Xin Qi, "Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unlimited Health Care Services (BC IoMT U6 HCS)," IEEE Access, vol. 7, pp. 31055-31066, 2019.

[4] G. Wu, S. Wang, Z. Ning, and B. Zhu, "Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5, pp. 1917-1927, May 2022.

[5] A. Shahnaz, U. Qamar, and A. Khalid, "Using Blockchain for Electronic Health Records," IEEE Access, vol. 7, pp. 134888-134902, 2019.

[6] R. G. Sonkamble, Phansalkar, S. P., Potdar, V. M., & Bongale, A. M. “Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR”. IEEE Access, 9, pp. 157558-157570,2021.

[7] R. P. Pinto, B. M. C. Silva, and P. R. M. Inácio, "A System for the Promotion of Traceability and Ownership of Health Data Using Blockchain," IEEE Access, vol. 10, pp. 139510-139523, 2022.

[8] S. Niu, L. Chen, J. Wang, and F. Yu, "Electronic Health Record Sharing Scheme with Searchable Attribute-Based Encryption on Blockchain," IEEE Access, vol. 7, pp. 183134- 183147, 2019.

[9] Z. Pang, Y. Yao, Q. Li, X. Zhang and J. Zhang, "Electronic Health Records Sharing Model Based on Blockchain Checkable State PBFT Consensus Algorithm," in IEEE Access, vol. 10, pp. 102765-102773, 2022

[10] Matthias Mettler, "Blockchain Technology in Healthcare" Boydak Strategy Consulting AG Freienbach, Switzerland.

[11] Zainab Alhadhrami, Salma Alghfeli, Mariam Alghfeli, Juhar Ahmed Abedlla, and Khaled Shuaib, "Introducing Blockchain for Healthcare," College of Information Technology, United Arab Emirates University.

[12] Claude Pirtle, Jesse Ehrenfeld, "Blockchain for Healthcare: The Next Generation of Medical Records?" Springer Science + Business Media, LLC, part of Springer Nature 2018.

[13] Peng Zhang, Douglas C. Schmidt, and Jules White, "Blockchain Technology Use Cases in Healthcare," Vanderbilt University, Nashville, TN.

[14] Marko Holbl, Marko Kompara, Aida Kamisalic, Lili Nemec Z; atolas, "A Systematic Review of the Use of Blockchain in Healthcare," the University of Maribor, Faculty of Electrical Engineering and Computer Science, Maribor, Slovenia.

[15] Sergey Avdoshin, Elena Pesotskaya, "Blockchain Revolution in the Healthcare Industry," National Research University Higher School of Economics, Moscow, Russian Federation.

[16] Kwabena Owusu, "Trufield," trufield.com.

[17] Andreas Bogner, Arne Meeuw, Mathieu Chanson, "A Decentralized Sharing App running a Smart Contract on the Ethereum Blockchain," Research Gate, Conference Paper November 2016.

[18] Zhang, P. White, J. Schmidt, D.C., and Lenaz, "Applying Software Patters to address interoperability in Blockchain-based healthcare apps," arXiv preprint arXiv: 1706.03700, 2017.

[19] Middleton B., Bloomrosen M., Dente M.A., Hashmat B., Koppel R., Overhage J. M., Payne T. H., Rosenbloom S. T., Weaver C., Zhang J., "Enhancing patient safety and quality of care by improving the usability of electronic health record systems: recommendations from AMIA," Journal of the American Medical Informatics Association, 2013

[20] J. Eberhardt and S. Tai, ''On or off the blockchain? Insights on offchaining computation and data,'' in Proc. Eur. Conf. Service-Oriented Cloud Comput., Oct. 2014, pp. 11–45.

[21] D. Vujičić, D. Jagodić, and S. Randić, ''Blockchain technology, bitcoin, and Ethereum: A brief overview,'' in Proc. 17th Int. Symp. INFOTEHJAHORINA (INFOTEH), Mar. 2018, pp. 1–6.

[22] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F.-Y. Wang, ''An overview of smart contract: Architecture, applications, and future trends,'' in Proc. IEEE Intell. Vehicles Symp. (IV), Jun. 2018, pp. 108–113.

[23] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, ''Blockchain distributed ledger technologies for biomedical and health care applications,'' J. Amer. Med. Inform. Assoc., vol. 24, no. 6, pp. 1211–1220, 2017.

[24] M. S. Sahoo and P. K. Baruah, ‘‘HBasechainDB—A scalable blockchain framework on Hadoop ecosystem,’’ in Supercomputing Frontiers. 2018, pp. 18–29.

[25] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, ‘‘FHIRChain: Applying blockchain to securely and scalably share clinical data,’’ Comput. Struct. Biotechnol. J., vol. 16, pp. 267–278, Jul. 2018.