J Inf Process Syst, Vol.15, No.2, pp.239~250, April 2019
https://doi.org/10.3745/JIPS.04.0106

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Enhanced Security Framework for E-Health Systems using Blockchain

Mohan Kubendiran*, Satyapal Singh*, and Arun Kumar Sangaiah*

Abstract

An individual's health data is very sensitive and private. Such data are usually stored on a private or community owned cloud, where access is not restricted to the owners of that cloud. Anyone within the cloud can access this data. This data may not be read only and multiple parties can make to it. Thus, any unauthorized modification of health-related data will lead to incorrect diagnosis and mistreatment. However, we cannot restrict semi-public access to this data. Existing security mechanisms in e-health systems are competent in dealing with the issues associated with these systems but only up to a certain extent. The indigenous technologies need to be complemented with current and future technologies. We have put forward a method to complement such technologies by incorporating the concept of blockchain to ensure the integrity of data as well as its provenance.

Keywords

Blockchain, Cloud Computing, Data Integrity, Data Provenance, E-Health System

1. Introduction

Cloud computing is a technology that enables the ubiquitous and on-demand sharing of configurable resources [1] like network, storage, computing power, etc. Cloud computing, also known as "computing as you go", is used to turn any computer system into a decentralized architecture in which users can access different services. In addition to the daily evolution of stakeholders' number and beneficiaries, the imbalance between the virtual machines at data centers in a cloud environment impacts the performance as it decreases the hardware resources and the software's profitability [2]. The most efficient number of virtual machines can be allocated by ensuring equal load balancing and increasing the total number of allocations possible in serial or parallel mode [3]. Cloud computing is attracting all domains, and health care is not an exception. Data integrity is an aspect of paramount significance in the medical field where all information is delicate. E-health systems are ecosystems meant to provide health and medical services through the internet. Since healthcare data are being migrated to the cloud these days, the management of its security has become vital. Replication of data over multiple nodes is an indigenous method of dealing with a number of security issues associated with cloud computing [4].

A blockchain is a public database of records distributed over multiple peers on a network [5]. Its innate property of immutability allows it to work as a secure database. It is not only confined to 'Bitcoin'

Manuscript received July 31, 2018, first revision October 30, 2018; accepted January 21, 2018.
Corresponding Author: Arun Kumar Sangaiah (sarunkumar@vit.ac.in)
* School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India ({mohan.k, satyapal.singh2015, sarunkumar}@vit.ac.in)

anymore but has deeply rooted itself in other fields. One of such fields is e-health systems. The sensitivity of data associated with this field demands a congruent security mechanism. Blockchains provide this required solution. They can be used in almost every aspect of e-health systems from patient education to fighting counterfeit drugs [6].

However, the mere introduction of blockchain in this field is not sufficient. It should be supplemented with appropriate technologies. In heterogeneous wireless networks supporting multi-access services, one challenge is selecting the best network from among the possible heterogeneous connections and providing seamless service during handover for a higher Quality of Services (QoSs) [7]. The implementation of blockchain should be done in such a way as to enhance the reliance of patients on a publicly open ledger of information. Electronic medical records (EMRs) are important for an intelligent e-health ecosystem [8]. A multiple-cloud system poses even greater challenges in integrity verification though mechanisms have been introduced to alleviate the situation [9,10]. Web applications are indispensable in the software industry and continuously evolve, either meeting newer criteria and/or including new functionalities.

While dealing with the security implications of the blockchain in e-health systems, we will confine ourselves to the assurance of integrity and data provenance in these systems. Confidentiality and availability, the other two most important aspects of security, are beyond the scope of this paper. In addition to implementing the blockchain on a primitive e-health system to verify the integrity of data, we have also proposed a novel algorithm to ensure data provenance or in simple terms the authorized origin of data.

2. Related Works

The work in [11] presents to us the pros and cons, the features and limitations, and future opportunities in the field of blockchain-based health care technologies. It emphasizes the significance of interoperability in such systems alongside the accessibility of health records. It also advocates the criteria within which the services rendered by blockchain technology can be fully exploited. The most prominent use of blockchain is in verifying the information flowing within a system and authenticating the source of this information. It reveals the confinements of Blockchain technology in its inability to deal with voluminous data. It brings forth a concept of on-chain and off-chain data on the blockchain to promote its performance. On-chain data is directly stored onto the chain, like storing the relatively small medical records of patients, and off-chain data is composed of the huge medical files stored on a remote database with its reference stored on the chain. However, this distinction does not consolidate the given hypothetical concepts with any experimental implementation.

Ekblaw et al. [12] provide a framework for healthcare systems that provides the patients access to their medical records across different health organizations. The proposed system focuses on some of the critical aspects of data security like confidentiality, sharing, authentication and accountability. It deals with the issue of fragmentation of patient data across organizations. In order to provide such a facility, it also tries to eliminate the interoperability challenges involved with it. The prime focus of this proposed architecture is to make the patient's authority over his data of paramount significance. The medical records of different organizations are allowed to be stored at different locations in their own databases with a copy of the reference data stored on each of the participating organizations' systems. However, it fails to take into

consideration the security of data for its participating parties.

Kuo et al. [13] present a comparison between the blockchain and indigenous distributed databases in the context of healthcare applications. Some of the benefits that it mentions include decentralized management, immutable audit trail and data provenance. Using these attributes of the blockchain technology as grounds, the paper advocates its uses in medical applications like patient consent records, patient health records, etc. It portrays the use of blockchain as distributed ledgers to store health associated data. In addition to simply acting as a store for data, blockchains can also be used in health information exchange such as the transfer of health-related data between patients and hospitals. Besides, they can also store genomic data, patient related outcomes data, etc. It further sheds light on the challenges of blockchain technology. Two issues are presented in the paper: transparency and confidentiality. But it does not address issues associated with the integrity of health-related data.

Dubovitskaya et al. [14] present a framework for the management of healthcare data, emphasizing the sharing of such data. This proposed framework strives to ensure availability, privacy, security and access control over health-related data. The major challenge depicted in the paper is keeping the medical history of a patient up-to-date. It also advocates the promotion of health information exchange ecosystems for the secure, efficient and accurate sharing of patient data across various domains. It declares the pseudonymity provided by blockchain technology as a potential threat to the privacy of an individual participating in it. Confidentiality is ensured by the use of encryption of data using a secret key. Availability is guaranteed by migrating the whole architecture onto a cloud. However, the issues associated with the integrity of data at client level are left unaddressed.

Liu et al. [15] provide a reliable, efficient and secure mechanism for the exchange of medical records. They work with the issues of e-healthcare systems such as reliability, scalability, security and efficiency. The paper identifies traditional e-health systems as inclined towards the stakeholders rather than actual patients. The proposed architecture addresses the need for privacy of patient data. It combines the best of certain online services and peer-to-peer networking. The blockchain in the context of healthcare stores data related to billing, claims, etc. Such an architecture has a high fault tolerance. The digitization of healthcare resources like patient records enhances the speed of management of such data and services. The patients can control access to their data. They can specify viewing rights to be provided to others while viewing their data. The proposed framework makes use of artificial intelligence and machine learning alongside the blockchain for efficient decision making. However, the participating entities in the chain have to be certified by a third party.

Zikratov et al. [16] present the flaws associated with the already existing simple integrity verification algorithms in the cloud. Cryptographic hash functions reduce inputs of arbitrary or very large length to a short string of fixed length [17]. Their paper discusses the flaws in the Message Authentication Code algorithm for integrity verification as well as that of primitive encryption methods. The impotence of hash trees in verifying the integrity of large quantities of information is also discussed. The system follows the basic blockchain algorithm for block creation. It takes in the transactions and mines them into different blocks based on a time window. It stores the whole file on the blockchain. For the purpose of integrity verification, the file whose integrity needs to be verified is fetched from the chain. A previous copy of the hash of the file under scrutiny already exists. A hash of the file fetched from the Blockchain is generated and cross-verified with the already existing hash. However, storage concerns may arise due to the huge size of the blockchain.

Ora and Pal [5] deal with the issue of integrity by merging the features of the RSA encryption algorithm and the MD5 one-way hashing algorithm. In the proposed framework, the data is first encrypted using the RSA algorithm and then outsourced to the cloud. The hashing is done afterwards. Once the file has been encrypted, the public-private key pair associated with it is generated. The hashing is done on the cloud itself to keep it secure. The MD5 hashing algorithm is used for this purpose. A copy of the hash obtained for the file is sent back to the client for a further verification process. The task of verification is also performed on the cloud server. For verification, the client may issue a verification request to the server. However, the leakage of the private key may hamper security.

A framework is proposed in [14] for the management of healthcare data, emphasizing the sharing of such data. This proposed framework strives to ensure availability, privacy, security and access control over health-related data. The major challenge depicted in the paper is keeping the medical history of a patient up-to-date. The paper also advocates the promotion of health information exchange ecosystems for the secure, efficient and accurate sharing of patient data across various domains. It declares the pseudonymity provides by the blockchain technology as a potential threat to the privacy of an individual participating in it. The architecture is inclined towards dealing with data related to a specific medical issue: cancer. The data of a patient is stored off-chain so as to maintain the scalability and speed of the blockchain. Confidentiality is ensured by the use of encryption of data using a secret key. Availability is guaranteed by migrating the whole architecture onto a cloud. However, it does not address the issues associated with the integrity of data at client level.

3. Blockchain-based Enhanced Security Framework for E-Health Systems (BESFES)

The system consists mainly of individual nodes connected via a peer-to-peer network (P2P). These nodes constitute the cloud itself and store data in a distributed fashion. The nodes are simple computers that agree to participate in the network. The diagram represented in Fig. 1 is just a small representation of the overall architecture involving multiple such hosts taking part in the sharing of data and multiple such cloud platforms. The system is broadly divided into three modules, namely the Core Module, Client Authentication Module, and Client Verification Module.

The core of the system consists of the Aggregation Server and the Clients. The aggregation server serves the following purpose. The gateway component of the server receives the requests from all the participating clients of the blockchain system. It receives the hashes from all the clients within a particular time window and sends them to the aggregation component of the server for further processing. The aggregation component collects all the hashes received from the different clients corresponding to a particular time frame and hashes them pairwise. Such an aggregation of the hashes onto different levels creates a tree-like data structure called the Merkle Tree [18]. The term Merkle Root denotes the top of the tree. The aggregation server also creates signature tokens for each of the hashes sent by the clients.

The clients have the following job to perform in the system. Each client generates the hash of the file that needs to be involved in the blockchain. It passes the file through a hash function, here SHA-512, in order to generate a 64-byte unique id for that file. The client also introduces the 'Forced Error' into the file that it just sent to the server.

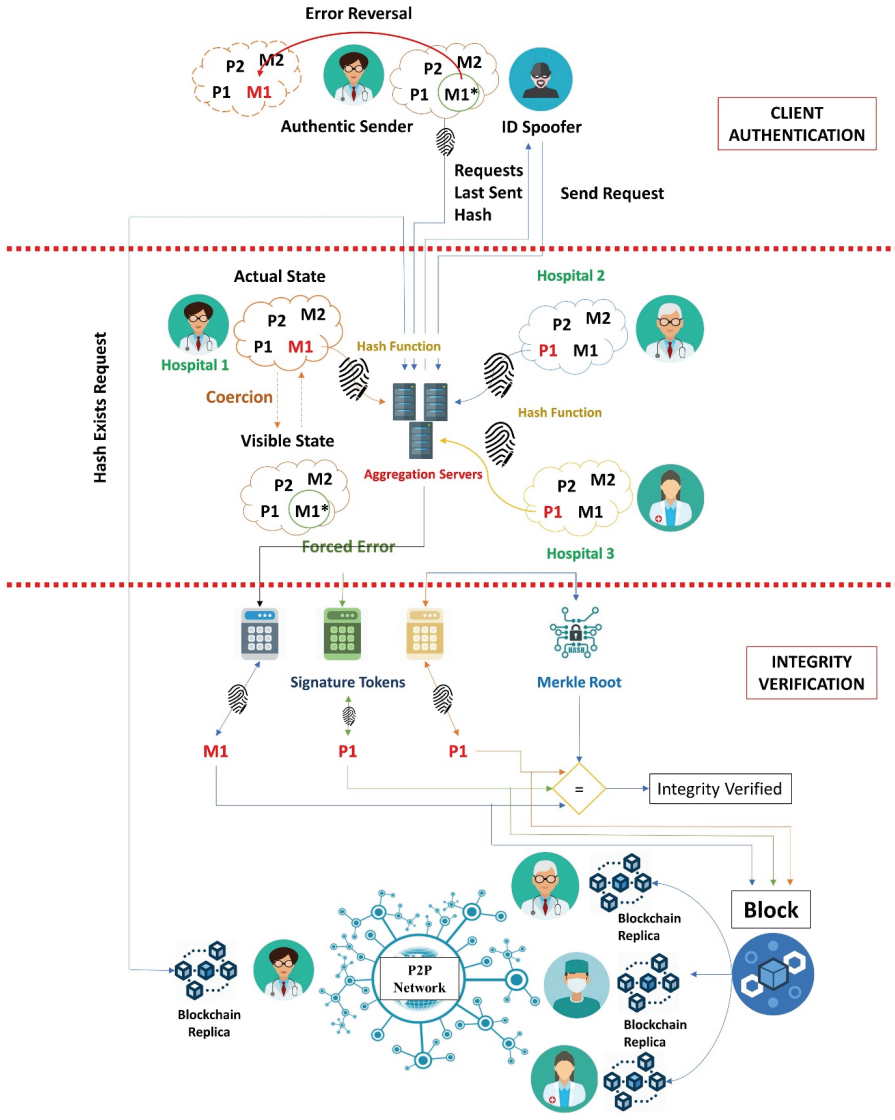

Fig. 1. Blockchain-based enhanced security framework for e-health systems (BESFES).

The client authentication module ensures that the client agent who sends the file to the server is indeed the one authorized to do so and not any malicious third party. Even the authorized users need to be differentiated amongst each other [19]. This module is responsible for ensuring data provenance. The client introduces a sort of error whenever he sends the file. This changes the state of the file in the cloud. The next time the same client tries to send a file, the server requests it to provide the hash of the last file that it sent. Since the error was explicitly introduced into the file, a spoofer will not know where the error was introduced into the file. In case the account of the authentic sender is stolen by the spoofer, he would still be sending the wrong hash to the server. The server cross checks the Blockchain for any such existing hash for that particular client's file. If not found, it will reset the connection with the client. In a valid process, the authentic client would reverse that error in the file, and then send it to the server. In this way, it could be ensured that only the authentic party is able to send the information even in the case of loss of

confidentiality of his/her account.

The integrity verification module verifies the integrity of any file on the client's side that has already been sent to the server. The process of verification is performed using the Merkle Root and the Signature Tokens already produced by the aggregation server. The aggregation server also provides a universal ID to the client for a file which is also used during the verification of that file. For any file to be verified, the hash of the file has to be created. The hash is then hashed with the hashes constituting the signature tokens for each of the client's hashes. The hashing is done in the exact order as it was done while forming the Merkle Tree. Hashing is not commutative, hence a change in the order of inputs to the hash function leads to a different output, resulting in a false positive. The final hash is then cross verified with the Merkle Root of the Merkle Tree. If both the hashes match, then integrity is verified. The hashes involved in that time frame are then mined into a block and added to the replicas of each of the client's blockchain.

4. Experimental Setup

A simulation of separate database stores for different hospitals' cloud systems was done by storing each of the hospital's data in distinct locations on the machine. Since all of them are on the same physical host, a separate P2P network does not need to be established explicitly. A java program to hash a file has been incorporated on the client's machine. A client-server architecture is used for the different hosts to send data to the aggregation servers for verification purposes. A piece of code written in java prepares the Merkle Tree with the help of the hashes of the files sent to the servers. The Merkle Root of each round is stored in a file on the server's side. The Signature Token is also generated and stored in a file on the server and used by the client for verification later on. The concept of linked list has been used to form a blockchain. The hash of a preceding block acts as the link to the next block where it is stored as a reference to the previous node alongside the current hash of the current node.

Secure hash algorithm (SHA) was used to generate 512-bit hash digests. The creation of finished blocks was followed by their storage on a ledger or a file. A timer was set at required positions to calculate the execution time of that particular part of program. For the purpose of comparison with other two works, a separate implementation of those works was performed. It was done in Java itself. For Work 1, the implementation of blockchain remained the same as ours while for the other work, RSA and MD5 algorithms were separately implemented and a timer was also added to keep a count of the time taken by the program for the verification of integrity.

All the calculations were done in approximation and the actual results may deviate from the ones provided here, but we have done our best to ensure that there is a minimum deviation in the outputs.

5. Comparative Analysis

A comparative analysis of the proposed framework was performed with the already existing frameworks as proposed in [6,7]. The analysis was done with respect to three attributes: time complexity, space complexity, and reliability of the algorithms.

The implementation was done wherever possible for the best comparison among the three algorithms. The comparison among the first two works was done in a conventional way as they are more or less based

on the same domain: blockchain. However, for comparison with the third work, we employed the help of some mathematical concepts.

5.1 Time Complexity

For comparing the time that the three algorithms in consideration would take to verify the integrity of files, four test scenarios were created. We considered healthcare associated files of four different sizes: 1 kB, 100 kB, 1 MB, and 100 MB (Fig. 2).

We ran the three algorithms on the different files one by one and found the trend as shown in the given chart for the four given files. The nature of the graph obtained is shown in the following section.

5.1.1 Blockchain-based enhanced security framework for e-health systems

The time taken to verify the integrity of a file of any size is independent of it. This is because only the hash value of each file is stored on the blockchain, which is the ultimate value being used to do the cross verification of hashes for integrity. Therefore, irrespective of the size of the file, the size of the hash is always 512 bits. Hence, the time taken to verify the integrity remains more or less constant in our algorithm.

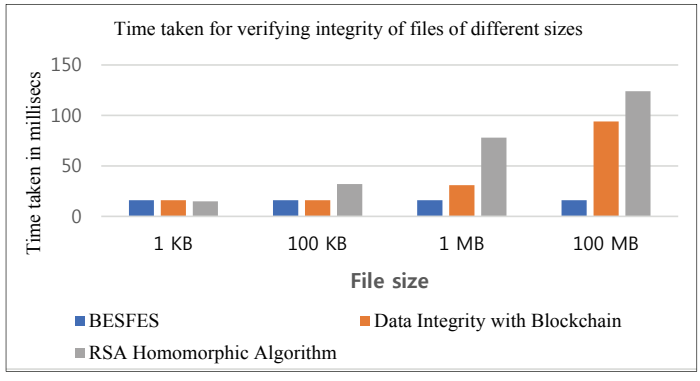

Fig. 2. Graph depicting the comparison of three algorithms.

5.1.2 Ensuring data integrity using blockchain technology

The approach of this algorithm is more or less the same as ours, but unlike ours it recomputed the hash of the files stored in the database for scrutiny. This results in an increased processing time with respect to increasing file sizes.

5.1.3 Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography

This method was observed to work fine with files of smaller sizes, but larger files require an increased number of parts into which it is divided, each part producing a fixed-length homomorphic encrypted output. Thus, to verify the integrity of the whole file, its different encrypted parts have to be accumulated, which results in an even larger chunk of data.

5.2 Space Complexity

For the comparison of space occupied by each unit of storage in the depicted works, we considered two valid transactions. It is assumed that these transactions are the only relevant subjects for the verification of integrity. Our work and Work 1 consider blockchain technology and hence need to be compared on the basis of block space.

5.2.1 Blockchain-based enhanced security framework for e-health systems

A simple block in our algorithm consists of the following Table 1.

Hence, the total space occupied by a block consisting of two transactions is 2656 bits.

Table 1. Components of a block

Parameter	Value
Block number	32 bits
Merkle Root	512 bits
Nonce	32 bits
Previous Hash	512 bits
Current Hash	512 bits
Timestamp	32 bits
Data	2 (no. of transactions) × 512 bits

5.2.2 Ensuring data integrity using blockchain technology

The second work follows the same approach as ours and hence the size of its block is around 2656 bits, for two transactions (Fig. 3).

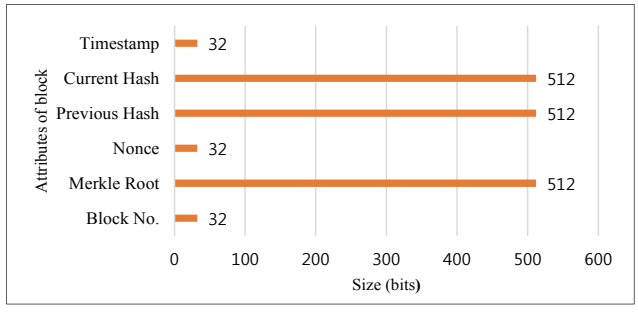

Fig. 3. Graph showing size of unit block.

5.2.3 Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography

Let us consider those two-transactional files of 512 bits each. For the sake of comparison, we will consider that the transactions are solely relevant for integrity check in this algorithm. Let these transactions be encrypted with a 256-bit key using PKCS1 padding. The maximum size of data that this RSA algorithm can encrypt simultaneously is the size of the key minus the size of the padding. Hence, the maximum size is equal to 245 bits. Now, to encrypt the two 512-bytes transactions, they need to be split

into two chunks of 245 bits each and an additional third chunk of 22 bits. The size of the encrypted output formed by the RSA algorithm is always equal to the size of the key used irrespective of the size of the data to be encrypted. Hence, the size of one encrypted transaction comes out to 768 bits. Therefore, it would require at least 1536 bits to contain two transactions in the system proposed by this work. However, if we consider the above two algorithms, the actual size of two transactions is found to be 1024 bits (Fig. 4).

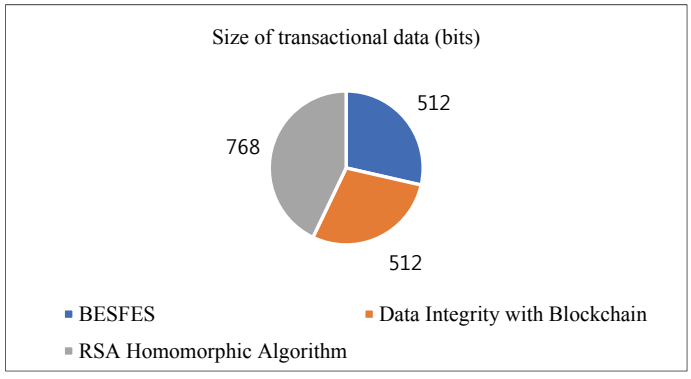

Fig. 4. Graph showing size of unit transactional data.

5.3 Reliability

5.3.1 Blockchain-based enhanced security framework for e-health systems

The architecture proposed in this paper provides a simple solution to both the problem of private key leakage as well as data provenance, reducing the risk involved compared to the other methods of data security. Considering the secrecy of private keys as the determining factor for the reliability of a system, let us assume that this system is used by a sample population of 100 people. Out of these 100 people, it is possible that only some of the users lose the privacy of their secret keys. Let us assume this number to be 10. Now, the reliability of the system would come to be 90%.

5.3.2 Ensuring data integrity using blockchain technology

If the encryption and decryption keys are leaked or the storage administrator colludes with some malicious attackers, then the system may start acting anomalously under the influence of the attacker. Out of 100 administrators, it is very possible that around 50% resort to malicious activities. Hence, the reliability ratio would be around 30% in the worst case scenario.

5.3.3 Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography

While verifying integrity, the system generates the hash of the file stored on the server and verifies it against the one already on the chain. This is a naïve method as there is no way of differentiating between an authorized or an enforced change in the file. Again, in this scenario, let us assume 100 users are using this system. It is very possible that the secret access key of the users is hijacked by a malicious user. The probability of this happening would be around 50% (Fig. 5).

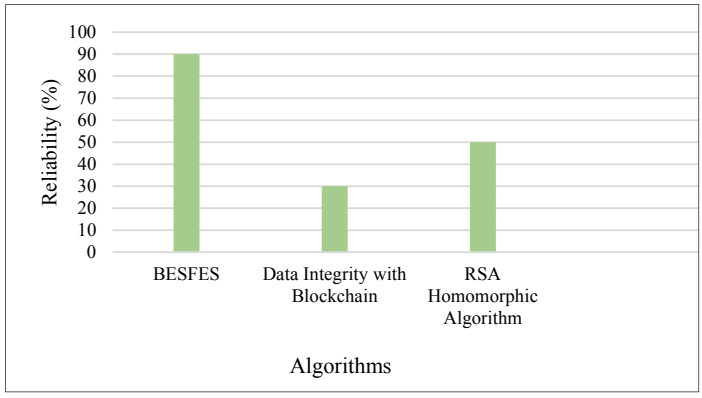

Fig. 5. Reliability of the three algorithms.

6. Conclusion

Data integrity has become a major issue and a point of vulnerability when the security issues related to data on the cloud are taken in to consideration, especially in the medical field. It is also important that access control to such sensitive data is strictly enforced. The involvement of third parties in providing such features is neither reliable nor sufficient. Amidst all these threats, the security of data on the healthcare systems' cloud requires an immutable and invulnerable technology. Blockchain is the answer to this. It is a public ledger, hence it provides all the transparency in the world. It is resistant to any kind of manipulation. The best way to provide security for data on the cloud is replicating it over multiple different networks. Blockchain does exactly this. No storage is required, and instead the data is stored in the form of blocks in a blockchain over multiple different nodes throughout a P2P.

In this work, we have presented a framework where blockchain could be efficiently used in e-health care systems for the verification of integrity of data. Furthermore, we presented a novel concept to ensure data provenance as it could be vital in the domain of healthcare. We considered two existing algorithms for ensuring data integrity and performed a comparative analysis with the experimental setup described above. It was found that our algorithm worked more effectively overall. In this paper, we have proposed a new partition-based device discovery scheme in shared controlled networks. In the proposed scheme, all devices are divided into several partitions. In addition, to avoid collisions occurring due to multiple responses, each device sends a response message based on a response timer that is configured by the controller.

From the numerical analysis, we can see that the proposed scheme can provide a much lower data discovery time than the existing schemes. Moreover, the performance gaps between the existing and proposed schemes become larger as the volume of data increases.

References

[1] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *AMIA Annual Symposium Proceedings*, Washington, DC, 2017, pp. 650-659.

[2] Y. Fahim, H. Rahhali, M. Hanine, E. H. Benlahmar, E. H. Labriji, M. Hanoune, and A. Eddaoui, "Load balancing in cloud computing using meta-heuristic algorithm," *Journal of Information Processing Systems*, vol. 14, no. 3, pp. 569-589, 2018.

[3] Y. S. Jeong and J. H. Park, "Novel solutions and approaches to effective data processing," *Journal of Information Processing Systems*, vol. 14, no. 3, pp. 563-568, 2018.

[4] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments," in *Proceedings of the Italian Conference on Cybersecurity*, Venice, Italy, 2017.

[5] P. Ora and P. R. Pal, "Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography," in *2015 International Conference on Computer, Communication and Control (IC4)*, Indore, India, 2015, pp. 1-6.

[6] M. Mettler, "Blockchain technology in healthcare: the revolution starts here," in *Proceedings of 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Munich, Germany, 2016, pp. 1-3.

[7] D. Pandey, B. H. Kim, H. S. Gang, G. R. Kwon, and J. Y. Pyun, "Maximizing network utilization in IEEE 802.21 assisted vertical handover over wireless heterogeneous networks," *Journal of Information Processing Systems*, vol. 14, no. 3, pp. 771-789, 2018.

[8] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of Medical Systems*, vol. 40, article no. 218, 2016.

[9] Y. Zhu, H. Hu, G. J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 12, pp. 2231-2244, 2012.

[10] C. Sasikala and C. S. Bindu, "A study on remote data integrity checking techniques in cloud," in *Proceedings of 2017 International Conference on Public Key Infrastructure and its Applications (PKIA)*, Bangalore, India, 2017, pp. 43-48.

[11] R. J. Krawiec, D. Housman, M. White, M. Filipova, F. Quarre, D. Barr, et al., "Blockchain: opportunities for health care," Deloitte Development LLC, 2016.

[12] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for Blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data," in *Proceedings of the 2nd International Conference on Open & Big Data*, Vienna, Austria, 2016.

[13] T. T. Kuo, H. E. Kim, and L. Ohno-Machado, "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.

[14] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," *AMIA Annual Symposium Proceedings*, vol. 2017, pp. 650-659, 2017.

[15] W. Liu, S. S. Zhu, T. Mundie, and U. Krieger, "Advanced block-chain architecture for e-health systems," in *Proceedings of 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Dalian, China, 2017, pp. 1-6.

[16] I. Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev, and L. Yalansky, "Ensuring data integrity using blockchain technology," in *Proceedings of 2017 20th Conference of Open Innovations Association (FRUCT)*, St. Petersburg, Russia, 2017, pp. 534-539.

[17] E. Andreeva, B. Mennink, and B. Preneel, "Security properties of domain extenders for cryptographic hash functions," *Journal of Information Processing Systems*, vol. 6, no. 4, pp. 453-480, 2010.

[18] A. Buldas, A. Kroonmaa, and R. Laanoja, "Keyless signatures' infrastructure: how to build global distributed hash-trees," in *Nordic Conference on Secure IT Systems*. Heidelberg: Springer, 2013, pp. 313-320.

[19] P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, "Metrics for assessing blockchain-based healthcare decentralized apps," in *Proceedings of 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Dalian, China, 2017, pp. 1-4.

Mohan Kubendiran https://orcid.org/0000-0001-5736-8525

He is working as an Associate Professor in School of Computer Science and Engineering (SCOPE) in Vellore Institute of Technology (VIT), Vellore, India. His area of interest includes cloud computing, e-health system, Internet of Things, big data analytics and information security.

Satyapal Singh https://orcid.org/0000-0003-3574-6454

He is an undergraduate student in School of Computer Science and Engineering (SCOPE) in Vellore Institute of Technology (VIT), Vellore, India. His area of interest includes virtualization and security in cloud.

Arun Kumar Sangaiah https://orcid.org/0000-0002-0229-2460

He is working as an Associate Professor in School of Computer Science and Engineering (SCOPE) in Vellore Institute of Technology (VIT), Vellore, India. His current research work includes global software development, wireless ad hoc and sensor networks, machine learning, cognitive networks and advances in mobile computing and communications.