Available online at www.sciencedirect.com

ScienceDirect

Cognitive Systems Research 52 (2018) 1–11

Cognitive Systems RESEARCH

www.elsevier.com/locate/cogsys

A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform

Ahmed F. Hussein [a,*], N. ArunKumar [b], Gustavo Ramirez-Gonzalez [c], Enas Abdulhay [d], João Manuel R.S. Tavares [e], Victor Hugo C. de Albuquerque [f]

[a] *Bio-Medical Engineering Department, Faculty of Engineering, AL-Nahrain University, Baghdad 10072, Iraq*
[b] *Department of Electronics and Instrumentation, SASTRA University, Thanjavur 613401, India*
[c] *Department of Telematics, University of Cauca, Colombia*
[d] *Faculty of Engineering, Department of Biomedical Engineering, Jordan University of Science and Technology, Jordan*
[e] *Instituto de Ciência e Inovação em Engenharia Mecânica e Engenharia Industrial, Departamento de Engenharia Mecânica, Faculdade de Engenharia, Universidade do Porto, Porto, Portugal*
[f] *Graduate Program in Applied Informatics, University of Fortaleza, Fortaleza, CE, Brazil*

Received 26 March 2018; received in revised form 18 April 2018; accepted 23 May 2018
Available online 30 May 2018

Abstract

The privacy of patients is jeopardised when medical records and data are spread or shared beyond the protected cloud of institutions. This is because breaches force them to the brink that they start abstaining from full disclosure of their condition. This type of condition has a negative effect on scientific research, patients and all stakeholders. A blockchain-based data sharing system is proposed to tackle this issue, which employs immutability and autonomy properties of the blockchain to sufficiently resolve challenges associated with access control and handle sensitive data. Our proposed system is supported by a Discrete Wavelet Transform to enhance the overall security, and a Genetic Algorithm technique to optimise the queuing optimization technique as well. Introducing this cryptographic key generator enhances the immunity and system access control, which allows verifying users securely in a fast way. This design allows further accountability since all users involved are already known and the blockchain records a log of their actions. Only when the users' cryptographic keys and identities are confirmed, the system allows requesting data from the shared queuing requests. The achieved execution time per node, confirmation time per node and robust index for block number of 0.19 s, 0.17 s and 20 respectively that based on system evaluation illustrates that our system is robust, efficient, immune and scalable.

Keywords: Blockchain; Cryptography; Genetic Algorithm; Discrete Wavelet Transform; Medical database management; Decentralised processing

1. Introduction

The electronic medical records or data related to the diagnosis and treatment of patient are considered extremely sensitive and private information. Consent data of patients are distributed across different controls as lifecycle events, which allow taking them away from one data provider to other (Cartwright-Smith, Gray, & Thorpe, 2016). This type of information is normally shared among peers such as clinics, hospitals, healthcare providers, researchers, insurance companies, healthcare centres

* Corresponding author.
E-mail address: ahmed.f.h.1976@gmail.com (A.F. Hussein).

https://doi.org/10.1016/j.cogsys.2018.05.004
1389-0417/© 2018 Elsevier B.V. All rights reserved.

and patient's families. This implies a serious challenge to safeguard these valuable data as well as updating the medical history of the patient. These information between multiple units need to be saved and shared, as the patient's treatment process could be hindered if multiple access control over numerous users is not enabled (Health, Staff, & Register, 2005; Meng, Tischhauser, Wang, Wang, & Han, 2018). The access to a full patient data history is very critical to continue his treatment, particularly for long-term treatment cases such as cancer patients, cardiovascular patients or HIV patients, and requires knowing the laboratory results, the medication doses or medicines' negative side effects. The patient may also be required to visit different medical institutions for consultation, or may even get transferred from one hospital to other, and to execute such an action, sharing of the patient's clinical data is mandatory for the treatment purposes. Coordination becomes more difficult, especially when a patient moves to another region, city or a country and is unsure of the hospital or caregiver where he will be receiving the treatment. The data sharing features allows the medical research institute to better understand, make the collaboration seamless between various healthcare providers and facilitate secure sharing with standard regulations (Yang, Li, & Niu, 2015).

Challenges associated with data processing, privacy and security continue to rise concurrently, since the healthcare industry highly relies on the data. Health data privacy implies securely and privately processing of the patient data or the need for authorisation to access the data. Besides, security refers to safeguarding sensitive data from intruders and even listeners (Al Omar, Rahman, Basu, & Kiyomoto, 2017). By giving the required tool to establish consensus among spread entities without depending on a single reliable party, the blockchain technique will ensure the data security, the control over sensitive data, and will facilitate healthcare data supervision for the patient as well as different actors in medical area (Dorri, Steger, Kanhere, & Jurdak, 2017; Sachs, 2016). As per Brodersen et al. (2016) 'Blockchains can be defined as cryptographic protocols that allow maintaining a shared ledger of information via a network of computers (nodes) collectively and a complete trust is not required amongst the nodes'. The blockchain methodology has helped understand numerous issues relating to the current health IT paradigms, involving immutably assuring expressed identities, security (specifically data integrity) and privacy, improving healthcare-related security for both patients and providers and creating highly robust audit trails. The private sector is aggressively experimenting by applying blockchain technology across the industries, including healthcare, owing to benefits like distributed ledger technologies (Fairley, 2017).

Moreover, multiple parties can share or maintain this distributed tamperproof database. Data can be stored in 'blocks' via the 'cryptography' technology so that only the intended users can open and view or read but not modify in case of integrity. The basic information security is ensured by cryptographic controls along with the information assurance trends (Di Vimercati, Foresti, Jajodia, & Samarati, 2007). A secret private key and a public key are maintained by each participant connected to the blockchain network, which also acts as an openly visible identifier. The pair is cryptographically linked in a manner that identification can be done only in one direction by making use of the private key. As such, a private key is necessary for anyone wishing to unlock a participant's identity to get access to the information on the blockchain as well as relevancy of the profile. Thus, in the future of the healthcare sector, a role for blockchain is certain. In fact, healthcare providers, technologists and professionals worldwide view blockchain technology as a significant tool for streamlining medical records sharing in a secured way to protect personal data (or privacy) of patients from hackers, outsiders and insiders, and provide patients with better control over their information (Sujansky, Faus, Stone, & Brennan, 2010; Wu, Zhang, Xie, Alelaiw, & Shen, 2017).

Developing a blockchain-based access control method is the need of the hour to sufficiently control the access to the stored medical data as well as allow processing on various systems to securely enable efficient data sharing. Secure cryptographic techniques are offered by the blockchain technology to authenticate and identify systems and users, thereby contriving access control in a distributed, secure and scalable method (Zyskind & Nathan, 2015). In such system, the blockchain is employed for data control, the system importance is denoted in Fig. 1 where all valuable medical data such as clinical history documentation is encrypted and secured.

This study proposes a scalable and robust system for managing the medical records and information. The

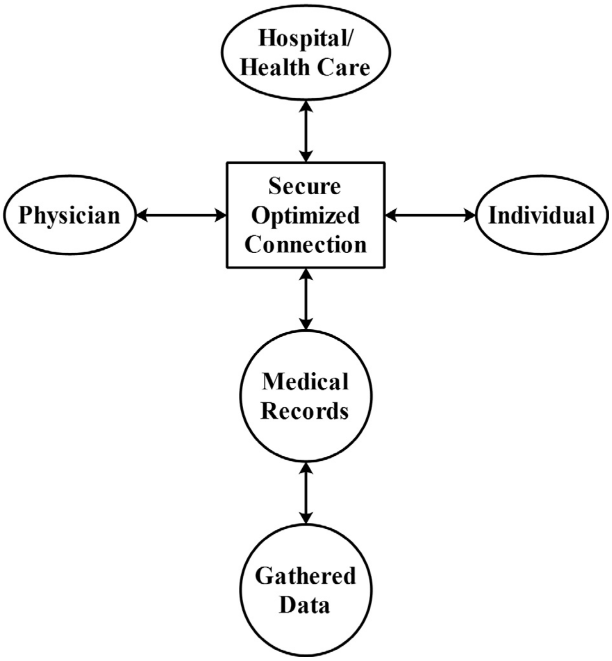

Fig. 1. The medical records system importance.

proposed system uses the blockchain technique as an access control method. This method employs a modified cryptography technique to maintain security as well as efficiency to easily get access control to sensitive medical data being shared. The modification uses the popularly known discreet wavelet transform to generate a new data sequence key (Hash function) via the traditional cryptographic method. Moreover, it is employ the Genetic Algorithm (GA) technique to reduce the transaction node time for selecting the data requests and improve the reliability as well. Besides, the using of Discrete Wavelet Transform (DWT) in Hash function generation process is contribute to improve the robustness. Also, the testing of redesigned blockchain data sharing system controlling the access of data users to their uniqueness and cryptographic keys has been done.

This paper is prepared in following way. Section 2 provides a literature review for related work, methods and techniques that used to implement the system. Section 3 describes in detail various methods for this work. The obtained results are presented and discussed in Section 4. While, the paper conclusion is presented in Section 5.

2. Literature review

2.1. Related work

The research challenges related to enhancing the blockchain technology have been described and presented.

Al Omar et al. (2017) put forward a data management system for patient healthcare, which employs blockchain to secure privacy storage. This framework addresses the issue of losing control when storing encrypted data within the system. Besides, the framework will be immune in terms of data protective vulnerabilities by employing cryptographic function with blockchain.

Ibriq and Mahgoub (2007) were presented a new scheme for wireless sensors network (WSN) namely scheme Hierarchical Key Establishment Scheme (HIKES). The proposed scheme contains a base station that act as a central confidence authority and empowers arbitrarily nominated sensors to act as local trust establishments on its behalf the cluster members and issuing all secret keys.

Kershaw et al. (2018) improve an electronic based medical record reminder for screening process. This proposed reminder scheme shows the incremental rates of screening twofold especially for older patients.

A privacy preservation platform was put forward by Zyskind and Nathan (2015) by making use of third-party mobile services. The proposed platform permits users to modify the authorisations only if the policies of access control kept on the blockchain are followed. Three objects are included in the proposed decentralised platform: service providers, mobile phone users and the nodes maintaining the blockchain. Two types of transactions can be defined in the blockchain network: T_{data} for data storage and recovery and access time T_{access} for access control management. Data gathered through the mobile phone of the user is encrypted and stored off-blockchain; and in the public ledger, only the data hashes are stored. The data in a T_{data} transaction can be queried by both the user and service.

A new secured and effectual cluster based WSNs transmitting protocol was demonstrated by Kavya and Babu (2015). This proposed protocol adopts the Identity-Based digital Signature (IBS) to optimise the most suitable plane for execution time reduction.

Chinnaswamy and Sreenivas (2015) proposed a WSN system that can increase the network lifetime. The system method based on selecting the High Energy First (HEF) model for selecting the cluster head that can optimise the clustering policy.

Within the healthcare data sharing systems, Yue, Wang, Jin, Li, and Jiang (2016) briefly described the access control management. A one purpose-centric access control model was proposed by the authors. In this, two classes of data operators were recognised: r-users and p-users. The r-users are suggested to read raw data while p-users are suggested to acquire data regarding retrieving results. A requester has to make a transaction for every data request to get access to data for a specific category under a limited time period based on their need.

Mehmood, Umar, and Song (2017) proposed a new mechanism called Inter-Cluster Multiple Key Distribution Scheme for Wireless Sensor Networks (ICMDS) which allows the whole network securing. In ICMDS, two sensor node's authenticity security phases are implemented and used while communicating with the cluster head established. This can contribute to improve the system nodes and reduce the required processing time.

A framework that can provide secure key management within heterogeneous network was proposed by Lei, Ogah, Asuquo, Cruickshank, and Sun (2016). This framework is tested for guiding the autonomous vehicle. The security managers is a crucial key role in the framework that retrieve the vehicle leaving information, summarising block to dynamic keys and then run the rekeying process to vehicles within the same security domain.

An access control model based on capability is described in Hernández-Ramos, Jara, Marín, and Skarmeta Gómez (2016), in which the model was directly used on resource constrained devices, by employing a fully distributed security approach. Ye, Zhu, Wang, Malekian, and Qiao-min (2014) put forward a well-organised authentication and access control scheme that was built according to the perception IoT access control layer attribute. Also, for the IoT, a generic authorisation framework has been put forward in Seitz, Selander, and Gehrmann (2013). It supports elastic access and fine-grained control, by following the current Internet standards and access control solutions like Security Assertion Markup Language and eXtensible Access Control Markup Language.

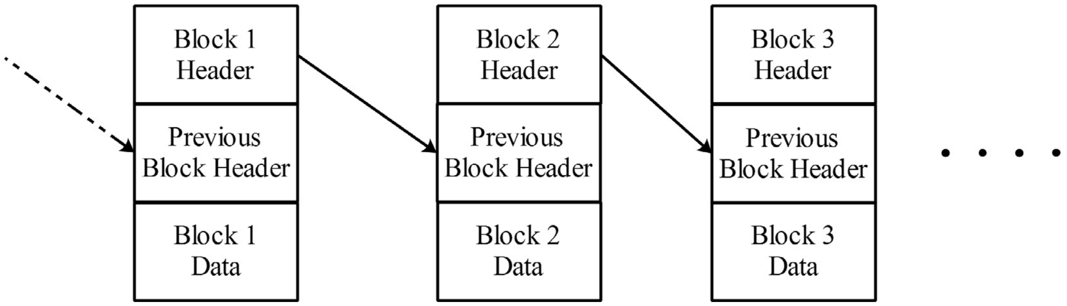

Fig. 2. Blockchain structure.

2.2. Blockchain network

As presented in Fig. 2, a blockchain can be defined as a decentralised computing architecture employed to cater to a growing list of ordered transactions that are grouped into blocks and are reconciled repeatedly to maintain up-to-date information. At a time, to the blockchain, just one block can be added and verification (using cryptography) is done for each block mathematically to guarantee that it follows the sequence from the previous block, thereby keeping consensus across the whole decentralised network. The verification process is known as Proof of Work (PoW) or "mining" (Nakamoto, 2008), which promotes completion amongst network nodes (also known as "miners") to become the first to have their block added in the next one to the Blockchain by resolving a puzzle that is computationally expensive. The solution is then broadcast by the winner to the entire network, which allows it to gain some mining rewards in crypto-currency. This mechanism integrates cryptography, the game theory and incentive engineering to allow the network reach a consensus concerning each block in the blockchain and ensure that there is no tampering with the transaction history. The blockchain stores all transaction records, which are shared with all network nodes. This allows maintain incorruptibility, transparency and robustness (as for failure, there is no single point) (Toyoda, Mathiopoulos, Sasase, & Ohtsuki, 2017).

Comparatively, the blockchain network is built from separate blocks that are moulded starting events chained along with the current or broadcast block to the origin block. The blocks are transmitted into the network after they catch events details information. Post that, the blocks get locked by forming a chain and can never be updated, reformed or removed. This also allows carrying out data forensics and improves data traceability in cases when there is a malicious threat in the system or where a user abuses the data handling policies in the group. A block is built from an individual event where an event can be defined as the time period when a request is created until when broadcasting of the block into the blockchain. For instance, when an authorised body has to examine system irregularities, a request is sent and then there is access grant to review into irregularities. For such irregularities, the consensus node is responsible for mining and reporting results. This is not very difficult since linking together of the blocks can be done with the blockchain's immutability property.

2.3. Discrete Wavelet Transform

In this study, a Discrete Wavelet Transform is employed for the cryptographic section to generate a unique hash decrypted key. In different engineering fields, wavelet transforms are broadly employed to solve several real-life problems. In Wavelet Transform (WT), to get a better-quality low frequency resolution, long-time windows are employed, while to get high-frequency information, short-time windows are employed. Therefore, precise time information and frequency information can be achieved via WT at high and low frequencies, respectively. This makes the WT optimum to analyse non-stationary, multi-component, and irregular data patterns, like impulses that may occur at different time instances. The continuous wavelet transform (CWT) of a signal $g(t)$ can be defined as the signal integral multiplied by shifted and scaled versions of a wavelet function *w,* which can be defined as follows:

$$CWT(a,b) = \int_{-\infty}^{\infty} g(t)\frac{1}{\sqrt{|a|}}\psi\left(\frac{t-b}{a}\right)dt \tag{1}$$

where a and b are termed as the scaling (frequency shared) and shifting parameters or time localisation, respectively (Burrus, Gopinath, Guo, Odegard, & Selesnick, 1998).

At every possible scale, calculating wavelet coefficients is deemed an expensive computational process. Instead, if the selection of shifts and scales is based on powers of two, also referred as dyadic scales and positions, then the efficiency of the wavelet analysis becomes greater. The DWT allows performing such analysis and can be defined as follows (Prabhakar, Mohanty, & Sekhar, 2002):

$$DWT(j,k) = \frac{1}{\sqrt{|2^j|}}\int_{-\infty}^{\infty} g(t)\psi\left(\frac{t-2^jk}{2^j}\right)dt \tag{2}$$

where 2^j a-nd 2^jk substitute a and b, respectively. A well-organized way to achieve this scheme was designed by Mallat (1989). He suggest to pass the tested signal via a sequence of high-pass (HP) and low-pass (LP) filter pairs called as quadrature structure mirror filters. In the DWT first step, simultaneous passion of the signal is done over LP and HP filters by maintaining a cut-off frequency of around one third of the sampling frequency. The outputs from these filters (LP and HP) are termed as calculation (A1) and element (D1) coefficients for the first level, correspondingly. According to Nyquist rule, the output signals can be down-sampled by two, which have half the frequency bandwidth of the original signal. For the first level approximation, the same procedure can be repeated and to get the second level coefficients, the detail coefficients are employed. At every step of this decomposition process, filtering is done to double the frequency resolution and down-sampling is done to halve the time resolution. Fig. 3 displays a signal's third level wavelet decay. In this demonstration, the frequency element of the original signal is represented by coefficients A1, D1, A2, D2, A3 and D3, g (n) signifies the HP filter and h(n) represents the LP filter of the original signal $f(n)$.

2.4. Cryptographic hash key

A mathematical representation of an algorithm is the cryptographic hash function that allows arbitrary size mapping data to a bit string that has a static size (a hash), that is also calculated to act as a unidirectional function, i.e. a function that is infeasible to invert (Miller, Juels, Shi, Parno, & Katz, 2014). Fig. 4 shows the hash function. Attempting a brute-force search for possible inputs is the only method to reconstruct the input data over an ideal cryptographic hash function's output to check if a match is produced, or if there is a need to use a rainbow table for matched hashes (Christidis & Devetsikiotis, 2016). According to B. Schneier, unidirectional hash functions are called as 'the modern cryptography workhorses' (Schneier, 2014). The message is most of the time the input data, while the output (the hash or hash value) is commonly known as the message digest or just the digest. The model cryptographic hash function can be characterised as: quick to compute the hash value, deterministic, changeable with original message changing, infeasible to generate a message from its hash value and non-redundant (impossible to determine if two different messages would generate the same hash value) (Lei et al., 2017; Thomas & Martin, 2006).

2.5. The Genetic Algorithm

The Genetic Algorithm (GA) technique is a group of computational processes model stimulated by evolution. This algorithm uses a chromosome-like data construction to find a potential and optimal solution for a given specific problem. The GA was first defined and developed by Holland (1992).

The GA processes can be explained in terms of selection, crossover and mutation procedures. The GA implementation starts with generates a random number strings set that known as population, that is composed a cluster of chromosomes. Fig. 5 describes the simple GA generation cycle, where this generation represents the optimum problem solutions. The components in the strings, which known as genes, are tuned to minimise or maximise the generated value of fitness function. The objective function should be wisely defined where it represents the specific problem. Then the chromosomes selection function is performed by selection operator. During the evolution process, the chromosome with accepted fitness value has a tremendous surviving chance, and it can be transferred from one set to another based on this value. The next implementation stage is a crossover operator. During this stage, chromosomes pairs are chosen randomly and generate two new issues. The crossover point is easily selected between the two parents' chromosome. After the crossover point selection, two new issues are produced. Finally, the chromosome bits value are randomly changed by mutation operator to keep GA from fast converting. This GA sequence is repeated continuously until reaching to the best solution (generations of the maximum number) as follow (Deb, Pratap, Agarwal, & Meyarivan, 2002; Moradi & Abedini, 2012):

$$N(h,t+1) \geqslant N(h,t)\frac{f(h,t)}{\bar{f}(t)}\left[1-p_c\frac{\delta(h)}{l-1}-p_m o(h)\right] \tag{3}$$

where

$f(h,t)$: is the schema h average fitness weight in generation t

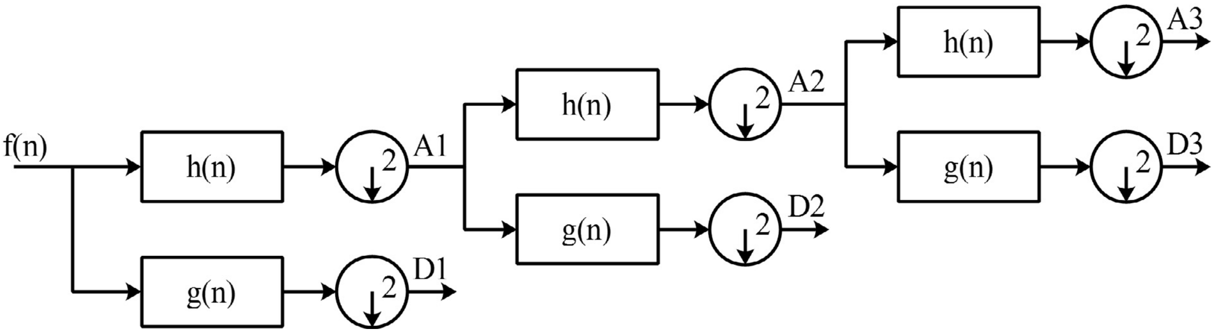

Fig. 3. Wavelet data decomposition.

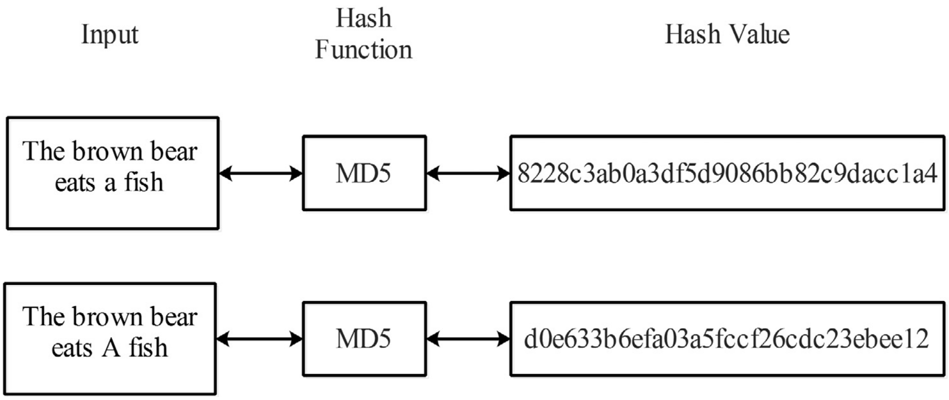
Input
Hash Function
Hash Value
The brown bear eats a fish
MD5
8228c3ab0a3df5d9086bb82c9dacc1a4
The brown bear eats A fish
MD5
d0e633b6efa03a5fccf26cdc23ebee12

Fig. 4. Hash function.

Population P1

String	Fitness Value
1000011111	0.6
0110100110	0.5
1111111110	0.9
0000011000	0.2

Population P2

String	Fitness Value
1010101011	0.6
1000011111	0.6
1111111011	0.9
1111111011	0.9

Fig. 5. The simple GA generation cycle.

$\bar{f}(t)$: is the population average fitness weight in generation t
p_c: probability of crossover
p_m: probability of mutation
$\delta(h)$: the total schema length
$o(h)$: the order of schema h
$N(h,t)$: the schema h expected instances number in generation t
l: the number of bit positions in string

3. Proposed system and methodology

Fig. 6 shows the proposed system architecture flow graph. It contains six main parts namely: network node, cryptographic hash generator, request queuing, GA operation, database and blockchain structure. A user key is generated by the cryptographic hash generator (CHG) when there is a need for fetching the new record for use. The key is shared equally with other network nodes as well. A user seeking to join this permission cluster needs to send a second request to the CHG. To confirm the user, the network node is tasked and permission is given to the user for joining this cluster or even deny user access. After the verification process is successfully completed, the CHG sends an acknowledgement to the user issuing the key. A key confirmation is requested by the user from the CHG by sending the key alongside a generated tag on entering the cluster. The CHG validates if the generation of the key was done correctly and sends a verification key to the user alongside few other parameters.

This study puts forward a modified encryption technique for implementing the cryptographic hash generator. For the encryption process, this modified technique employs the DWT to enhance the security level. Fig. 7 presents the CHG employing a popular encrypted hash generator called as MD5. The MD5 includes 64 of operation structure, which are clustered in four rounds of 16 operations. In each round a nonlinear function F is employed. M_i specifies the message input's 32-bit block, and K_i signifies a 32-bit constant, which vary for each operation. Left shifts represent a left bit rotation with s places; and for each operation, s would change (Balamurugan, Sivasubramanian, & Parvathavarthini, 2017; Wang & Yu, 2005). After converting the result from MD5 operation to numeric version, the DWT is applied to make use of the wavelet coefficients. The result then passes to implemented system in the form of a resultant key for employing it inside the presented system.

During the verification process, the private key is obtained from the CHG, which is used to create the request sent by the user. The operator makes use of the remote key to generate the block (request), signing the request via the private key of transaction and then send it to request queuing. Blocks are used to build the pool of unprocessed requests, which have not yet been processed through the consensus nodes. To validate a request, the request from the queue is supplied first to GA process to find the optimum request which then fetched by the consensus node

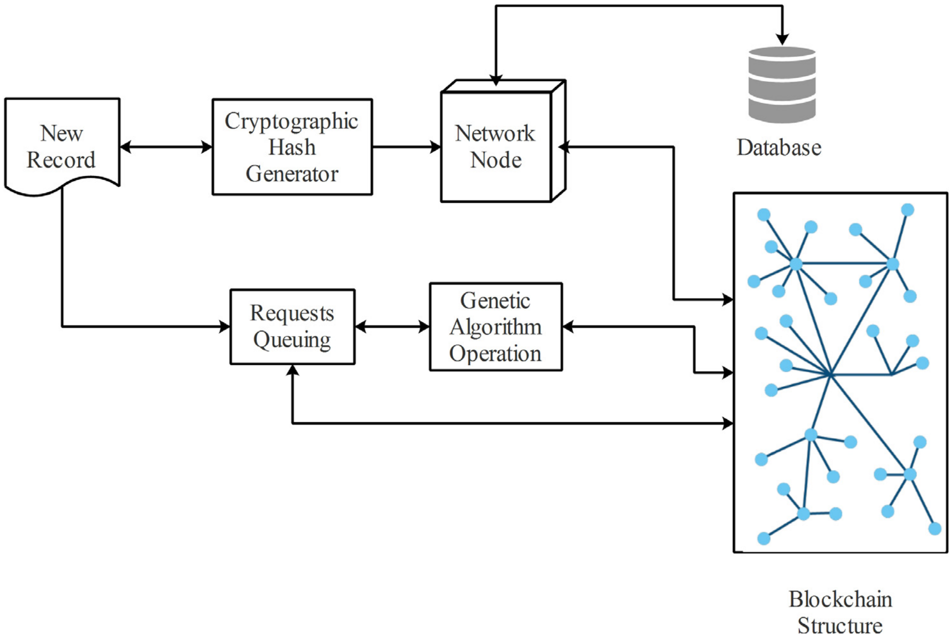

Fig. 6. The proposed system architecture.

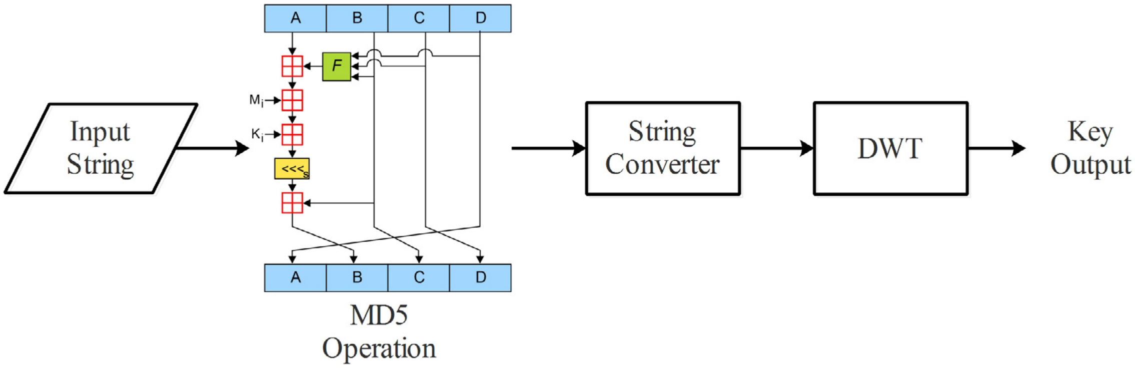

Fig. 7. The proposed cryptography hash generator.

to initiate the validation process. In this study, the GA parameters initially are set as follow: population size is 10, crossover rate is 0.5, and mutation rate is 0.01.

A block is built from a single event and an event can be defined as the time period when a request is created until when broadcasting of the block into the blockchain. For instance, when an authorised body has to examine system irregularities, a request is directed and then there is access granted to probe into abnormalities. For such irregularities, the consensus node is responsible for mining and reporting results. This is not very difficult since linking together of the blocks can be done with the blockchain's immutability property.

The block header ensures immutability and plays a key role in the blockchain network. If a block header is changed, an attacker needs to change all block headers ranging right from the start of the genesis block to falsify the record of a block. This helps in establishing security on the network as the assurance is maximum for the impossibility of achieving this task. Also, the system gets alerted if there is a block mismatch due to a suspicious on-going event and will trigger data forensics.

The version number is included in the block header showing the validation rules to follow. The previous block's hash is used to make the header, which is an MD5 hash and functions to ensure that there is no change in previous block header without altering the header of this block. This is done by considering all the hashes associated with the actions in the blockchain network and attaching the current block output. The block includes a transaction security that records the total transactions number occurring in the complete block. The transaction is built up with the user transaction and the consensus transaction that are associated with the purposes and processing of records as defined in the transaction section.

After accepting the request of a user, access is provided to the user related to the requested data or input, and then the verified request is considered ready for broadcast. This

Table 1
Key generation output.

The input (string)	MD5	Wavelet coefficient output
The first test	17cf8676b6da417ce732b3bf7177606e	836713788771071317898728661061318677709712866
The first test	8c172dfa16097e574b0ee72e1de0418c	1009784921508071102869310712588110125629912764
Patients name for testing issue	518ad3672c47c9aec62adba284ea82b6	68719712468977810912912012186149117681361089484
The yellow hornet bit the small child	f6d20f5a8c6b04a86d511d6a0baa0838	115127103881101091118210896859010910114680777869
Today, we have a party	2271427c619e227da0f77fa5d1e0ef05	7271746899841018198120105971251051011338369133

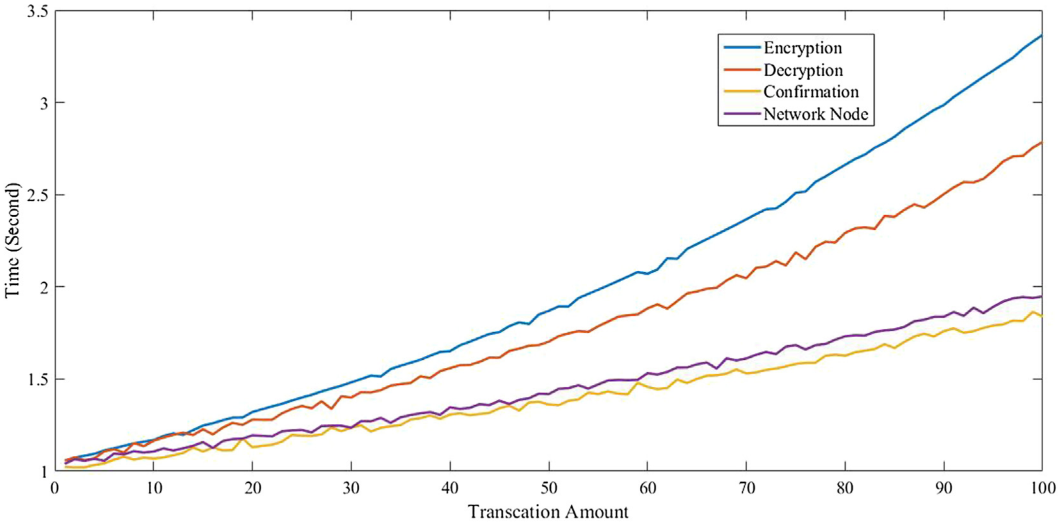

Fig. 8. The key transferring time procedure measurements.

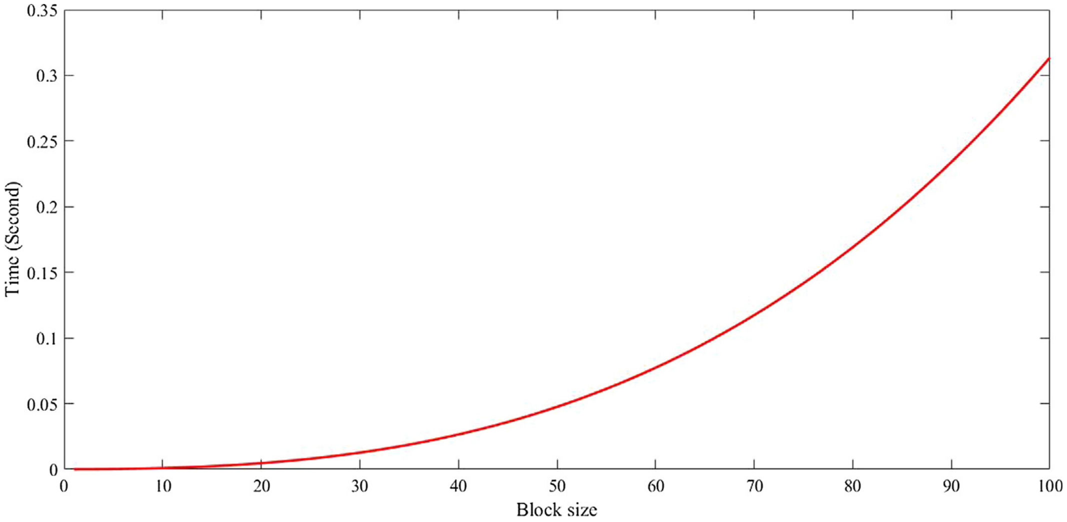

Fig. 9. The block generation required time.

is recorded via the consensus time for broadcasting with a record that has a purpose and the user apart for just creating this block. Then, a signature through verified processing proof is recorded. During the processing, the block's layer format is finished by attaching to a structure number of the generated format by employing the user key to detect the block mentioned current position. In the header, the block's version number is recorded as part of the processing. The header also records the hash of the previous block, thereby forming the Merkle root that also includes the current block. After formation of the header hash, the block for transmission becomes ready. At this time, an assurance can be given for the block regarding it being an essential of the blockchain network and as a part of the chain. Since now the block is a part of the chain system, in the blockchain system, it adds to the top blocks. For occurrences in which there is formation of other blocks after this block, the last header block's hash in the network is considered and appended to the newer block's header, which has not yet been a portion of the chained blocks in the system.

4. Results and discussion

The outcomes attained from the recommended blockchain-based system were subjected to simulations. The simulation scheme was executed with core i5 and 4 GB RAM powered by a dedicated GPU. Notably, the result computations have their basis in this hardware, where there is a likelihood of variance in the use of various hardware specifications.

Table 1 exhibits the outcomes of the different key generation phases. The MD5 and Wavelet coefficients generators form the primary key generation parts. The outcomes highlight the enhancement in the security level wherein the key generated is encoded a couple of times prior to utilising it inside the system. The produced key's fixed length can aid in decreasing the system intricacy and availability.

Fig. 8 depicts the time utilisation during various system schemes deployed for the key transferring procedure. The confirmation and network node processing time vary near linearly with the transaction payload or execution time. While the decryption and processing time vary non-linearly with the transaction payload and consume more time. This is likely when the encryption and decryption procedures carry average value from several simulation values. The payload measurements are figure out the effect of queuing requests on system efficiency, where the processing time may increases and pay the system to the extreme edge. To overcome this unwanted issue, the GA was used to optimise the request selection. This optimisation can assist the process flow and control the requests that ensure the overall stability.

Fig. 9 depicts the time needed for block generation. The requisite time goes up with the total number of blocks, and the overall process is augmented too. The block preparation required time increases exponentially with the growth of generated blocks. The generated block time slowly increased before 20, and the rapid time changing starts from 25. This observation indicate the importance of predefine the generated blocks in the system to get a better performance at lowest latency. The outcomes indicate a rapid block generation which signifies the optimisation system designing.

Fig. 10 exhibits how strong the recommended system is. The robustness index is gauged by calculating the total blocks which can hold valid transaction batches that are already encoded and hashed to Merkle tree to the overall blocks number. The outcomes indicate that the new

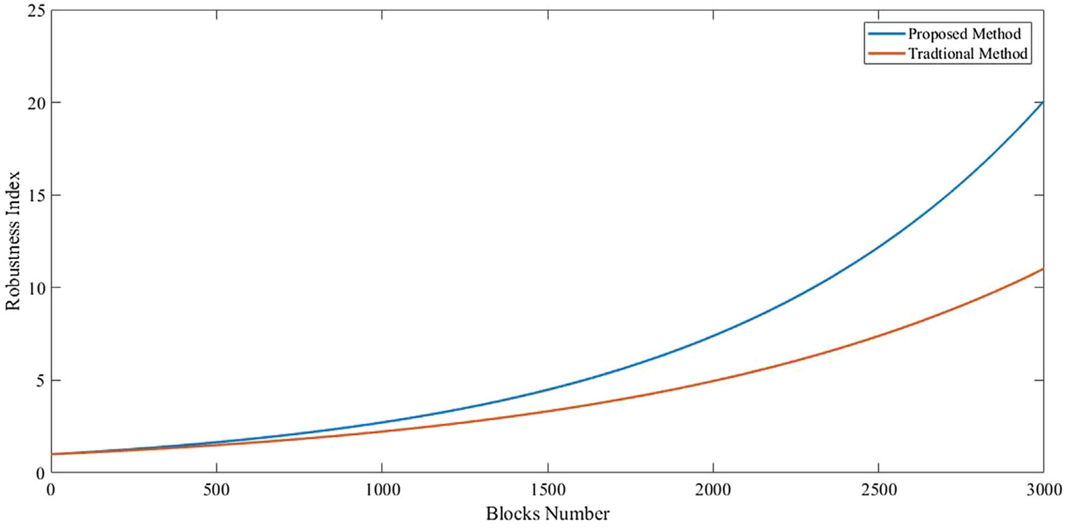

Fig. 10. Robustness measurements.

Table 2
Execution time benchmarking.

Scheme	Execution time per node (s)
Hierarchical key establishment scheme (Ibriq & Mahgoub, 2007)	0.38
High energy first (Chinnaswamy & Sreenivas, 2015)	0.36
Secure and efficient data transmission – identity based digital signature (Kavya & Babu, 2015)	0.41
Inter cluster multiple-key distribution (Mehmood et al., 2017)	0.33
Secure key management framework (Lei et al., 2016)	0.25
This work	0.19

recommended technique shows higher robustness in comparison to the conventional approach. The robustness factor is crucial in a blockchain-based system since the system dependability is reliant on the blocks produced.

The execution time benchmarking with other existing schemes is illustrated in Table 2. The comparison is based on execution time or system payload as an efficiency indicator to evaluate the total performance. Each system adopts different algorithm that fit the required requirements. The obtained results from benchmarking ensure the efficiency and reliability of proposed system for working under different environments and it can provide a satisfactory security protection.

5. Conclusions

This paper recommended a medical records managing and securing blockchain system. The system utilises a modified cryptographic hash generator for producing the necessary user security key. The recommended design deploys the discrete wavelet transform in the cryptographic generator part where it produces a new key format from MD5 strings. This alteration raises the general system security and increases its immunity to various kinds of attacks. The additional decryption phase can raise the processing time to some extent. Such increment is fine where the moving data's privacy matters. This study deploys several modes of assessment for testing the recommended system response against around variables. When a comparison is made of the attained outcomes and other blockchain-based systems, our recommended system exhibited higher scalability, robustness and immunity which enables secure data sharing and offers dependable data privacy. The recommended system can be utilised effectually for transferring the sensitive data during various working environments like clinics, hospitals, and healthcare centres. Going forward, the system can be controlled during cloud environment for greater expandability. This would help augment system resources and enhance the security.

Acknowledgement

Victor Hugo C. de Albuquerque received support from the Brazilian National Council for Research and Development (CNPq, Grant #304315/2017-6).

References

Al Omar, A., Rahman, M. S., Basu, A., & Kiyomoto, S. (2017). Medibchain: A blockchain based privacy preserving platform for healthcare data. In *International conference on security, privacy and anonymity in computation, communication and storage* (pp. 534–543).

Balamurugan, A., Sivasubramanian, A., & Parvathavarthini, B. (2017). Secured hash based burst header authentication design for optical burst switched networks. *Journal of Optical Communications, 38*, 433–438.

Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E., Truscott, A., et al. (2016). *Blockchain: Securing a new health interoperability experience*. Accenture LLP.

Burrus, C. S., Gopinath, R. A., Guo, H., Odegard, J. E., & Selesnick, I. W. (1998). *Introduction to wavelets and wavelet transforms: A primer* (Vol. 1). New Jersey: Prentice Hall.

Cartwright-Smith, L., Gray, E., & Thorpe, J. H. (2016). Health information ownership: Legal theories and policy implications. *Vanderbilt Journal of Entertainment & Technology Law, 19*, 207.

Chinnaswamy, C., & Sreenivas, T. (2015). Maximizing the lifetime and data security of WSNs using HEF algorithm and Paillier homomorphism. *International Journal, 3*.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access, 4*, 2292–2303.

Deb, K., Pratap, A., Agarwal, S., & Meyarivan, T. (2002). A fast and elitist multiobjective genetic algorithm: NSGA-II. *IEEE Transactions on Evolutionary Computation, 6*, 182–197.

Di Vimercati, S. D. C., Foresti, S., Jajodia, S., & Samarati, P. (2007). Access control policies and languages in open environments. In *Secure data management in decentralized systems* (pp. 21–58). Springer.

Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). Blockchain: A distributed solution to automotive security and privacy. *IEEE Communications Magazine, 55*, 119–125.

Fairley, P. (2017). Blockchain world-Feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous. *IEEE Spectrum, 54*, 36–59.

Health, D. o., Staff, H. S., & Register, O. o. t. F. (2005). *Code of federal regulations: Title 45: Public welfare*. United States Government Printing.

Hernández-Ramos, J. L., Jara, A. J., Marín, L., & Skarmeta Gómez, A. F. (2016). DCapBAC: embedding authorization logic into smart things through ECC optimizations. *International Journal of Computer Mathematics, 93*, 345–366.

Holland, J. H. (1992). *Adaptation in natural and artificial systems: An introductory analysis with applications to biology, control, and artificial intelligence*. MIT Press.

Ibriq, J., & Mahgoub, I. (2007). A hierarchical key establishment scheme for wireless sensor networks. In *21st International conference on advanced information networking and applications, 2007. AINA'07* (pp. 210–219).

Kavya, V., & Babu, G. P. (2015). Using multi-level encryption for efficient message transmission in cluster based WSNs. *International Journal, 3*.

Kershaw, C., Taylor, J. L., Horowitz, G., Brockmeyer, D., Libman, H., Kriegel, G., et al. (2018). Use of an electronic medical record reminder improves HIV screening. *BMC Health Services Research, 18*, 14.

Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal, 4*, 1832–1843.

Lei, A., Ogah, C., Asuquo, P., Cruickshank, H., & Sun, Z. (2016). A secure key management scheme for heterogeneous secure vehicular communication systems. *ZTE Communications, 21*, 1.

Mallat, S. G. (1989). A theory for multiresolution signal decomposition: The wavelet representation. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 11*, 674–693.

Mehmood, A., Umar, M. M., & Song, H. (2017). ICMDS: Secure inter-cluster multiple-key distribution scheme for wireless sensor networks. *Ad Hoc Networks, 55*, 97–106.

Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., & Han, J. (2018). When intrusion detection meets blockchain technology: A review. *IEEE Access, 6*, 10179–10188.

Miller, A., Juels, A., Shi, E., Parno, B., & Katz, J. (2014). Permacoin: Repurposing bitcoin work for data preservation. In *IEEE symposium on security and privacy (SP), 2014* (pp. 475–490).

Moradi, M. H., & Abedini, M. (2012). A combination of genetic algorithm and particle swarm optimization for optimal DG location and sizing in distribution systems. *International Journal of Electrical Power & Energy Systems, 34*, 66–74.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system, UNICAMP–IA368.

Prabhakar, S., Mohanty, A., & Sekhar, A. (2002). Application of discrete wavelet transform for detection of ball bearing race faults. *Tribology International, 35*, 793–800.

Sachs, G. (2016). *Profiles in Innovation: Blockchain–putting theory into practice*, May 2016.

Schneier, B. (2014). The Internet of things is wildly insecure—And often unpatchable. *Schneier on Security, 6*.

Seitz, L., Selander, G., & Gehrmann, C. (2013). Authorization framework for the internet-of-things. In *14th International symposium and workshops on a world of wireless, mobile and multimedia networks (WoWMoM), 2013* (pp. 1–6). IEEE.

Sujansky, W. V., Faus, S. A., Stone, E., & Brennan, P. F. (2010). A method to implement fine-grained access control for personal health records through standard relational database queries. *Journal of Biomedical Informatics, 43*, S46–S50.

Thomas, S., & Martin, J. (2006). Paradigm, workbook, and collection development.

Toyoda, K., Mathiopoulos, P. T., Sasase, I., & Ohtsuki, T. (2017). A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. *IEEE Access*.

Wang, X., Yu, H. (2005). How to break MD5 and other hash functions. In *Annual international conference on the theory and applications of cryptographic techniques* (pp. 19–35).

Wu, L., Zhang, Y., Xie, Y., Alelaiw, A., & Shen, J. (2017). An efficient and secure identity-based authentication and key agreement protocol with user anonymity for mobile devices. *Wireless Personal Communications, 94*, 3371–3387.

Yang, J.-J., Li, J.-Q., & Niu, Y. (2015). A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Future Generation Computer Systems, 43*, 74–86.

Ye, N., Zhu, Y., Wang, R.-C., Malekian, R., & Qiao-min, L. (2014). An efficient authentication and access control scheme for perception layer of internet of things. *Applied Mathematics & Information Sciences, 8*, 1617.

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems, 40*, 218.

Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *Security and privacy workshops (SPW), 2015* (pp. 180–184). IEEE.