Received May 4, 2020, accepted May 14, 2020, date of publication May 18, 2020, date of current version June 4, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2995481

A Privacy Preserving Distributed Ledger Framework for Global Human Resource Record Management: The Blockchain Aspect

TAI-HOON KIM[1], (Member, IEEE), GULSHAN KUMAR[2,3], RAHUL SAHA[2,3], MRITUNJAY KUMAR RAI[4], WILLIAM J. BUCHANAN[5], REJI THOMAS[3,6], AND MAMOUN ALAZAB[7], (Senior Member, IEEE)

[1]School of Economics and Management, Beijing Jiaotong University, Beijing 100044, China
[2]School of Computer Science and Engineering, Lovely Professional University, Phagwara 144411, India
[3]Division of Research and Development, Lovely Professional University, Phagwara 144411, India
[4]School of Electronics and Communication Engineering, Lovely Professional University, Phagwara 144411, India
[5]Blockpass ID Laboratory, Edinburgh Napier University, Edinburgh EH105 DT, U.K.
[6]School of Physical Science and Chemical Engineering, Lovely Professional University, Phagwara 144411, India
[7]College of Engineering, IT and Environment, Charles Darwin University, Casuarina, NT 0810, Australia

Corresponding authors: Mamoun Alazab (mamoun.alazab@cdu.edu.au) and Gulshan Kumar (gulshan3971@gmail.com)

This work was supported by the Department of Corporate and Information Services, NTG, Australia.

ABSTRACT Blockchain is a technology used with the series of users in peer-to-peer transactions to utilize the usability properties of the immutable data records. The distributed nature of this technology has given the wide acceptance to its range of applications in various sectors. Seeing the prospect of this new technology, we have chosen the field of human resource management as these data needs to be privacy preserving and confidential along with significant research value. Distributed ledger approach is a novel idea in this field of work specifically for the application of human resource records management. We have used a privacy preserving framework that provides a transparent system for human resource record management. Wallets are generated with organization id and outputting with public-private key pair along with privacy parameter mapping with hash. Keys are used to provide confidentiality, integrity and authentication. Smart contract uses distributed but converged decision with privacy level classification. Performance of the proposed work has been measured based on time, memory consumptions, failure point identification and read-write latencies. The analysis of the results confirms the efficiency of the system.

INDEX TERMS Blockchain, distributed ledger, human resource, management, privacy.

I. INTRODUCTION

The present computing technology has shifted its paradigm from centralized to the distributed one. With the increasing need of trust, comfort and transparency, blockchain has marked its presence in this field of distributed computing by the introduction of cryptocurrency 'Bitcoin' [1]. The need of ever felt transparency has been finally proved by blockchain since then. Therefore, to embrace this efficiency of distributed and transparent system, all the fields of operations in organizations are trying their best to identify the applicability of blockchain technology [2], [3]. The evolving applications around blockchain and distributed systems also make it a candidate for technology innovations [4]. Commercialization of blockchain technology in various fields also makes the pathway of its wide acceptance [5]. Moreover, the advent of IoT based network infrastructures, e-commerce and different spheres of quality of services demand for transparent and reliable solution of access and accountability [6], [7]. Therefore, we have made our objective to apply the distributed ledger in managing the human resource record to provide a successful human-resource-management system based on blockchain.

Human resource is an integral and core part of all the organizations. With the various background, ethnicity,

The associate editor coordinating the review of this manuscript and approving it for publication was Honghao Gao.

sex and racial features employees work with their ability of working. To hire these employees for an organization, rigorous recruitment processes are executed which include different mathematical, philosophical and statistical approximation models [8]. For example, multilevel structure [9], [10] and new axiomatic principle is worth of mentioning here [11]. These are also followed by various organizations depending upon their staffing structure [12]. Human resource management with different phases and different scope and viability therefore makes it a concerning point of involvement [13], [14]. However, the valid process of recruitment is missing from the organizations where the newly recruited employee produces fake or falsified background information to pass through the recruitment selection procedures, especially the academic background and previous working experience [15]. Organization dynamics also lead to the human resource acquisition which is a momentum factor for any loss or profit of the organization [16], [17]. As a result, various social engineering or related technical attacks and management dishonour are faced by the organization.

Moreover, for the social impact analysis and educational purposes, these data of the employees are shared among third parties [18]. Every organization follows a contract of privacy settlement and the agreement of privacy preservation with the clause of sharing the required data of the employees [19], [20]. For example, Health Insurance Portability and Accountability Act of 1996 (HIPAA) ensures the privacy of medical information [21]. Holding the hand of blockchain technology, IoT is being expanded for various industrial solutions with big data maintaining the privacy [22]. Now-a-days such social imaging is more often for recruiting employees. Considering the career networking as a part of social event, such privacy is required in social networking while recruiting or searching for jobs on various web portals [23], [24]. Furthermore, we refrain ourselves to post check those clauses and agreements to verify the privacy preservation processes. As a result, trust issues make a challenge for the organization. Therefore, to ensure the privacy along with the proper verification and validation of the employee background, a human resource management system is need of the technology which have transparent and distributed verification and validation provision. Though organizations are excited about using the clouds but the technology shift to the clouds for middle and small level organizations still pending due to various challenges [25], [26].

In the existing human resource record management process the task and activities are maintained manually. The verification of records is done based on the availability of previous records and sources. Moreover, organizations are not confirmed/assured about the employees currently under consideration. For example, employee E is working in company ABC. Due to some act of mismanagement of tasks or even dishonesty the employee has been fired from the job. Now, if the same employee wants to get into another organization XYZ with same psychological or behavioural attributes it may be a risk for the organization XYZ to recruit the employee E as it may again do misleading works against the rules and regulations of the organization. Such things are unverifiable in the existing human resource management system. Moreover, the credentials that the employees provide at the time of interview, there is no transparent process for their verification. As a result, various fake data are acknowledged and later the organization faces problems. This rationale is a motivation for the present work.

Blockchain based solution for managing such processes are therefore going to be beneficial at the present time. The inclusion of blockchain with distributed ledger for human resource management is advantageous for the organizations to maintain the Human Resource Records (HRRs). Therefore, in this paper, we have shown a privacy preserving blockchain approach to converge the use of HRRs on the global platform.

The rest of the paper has been organized as following. Section II discusses the background of blockchain technology and recent applications. Section III proposes a distributed ledger framework for the feasible application in human resource records management. Section IV explains the feasibility of the model and its advantages. The performance results are shown on section V. Logical conclusion has been drawn in section VI.

II. BACKGROUND OF BLOCKCHAIN AND RECENT STUDY

A. FUNDAMENTALS OF BLOCKCHAIN

Blockchain is transitive with logical chaining process. It uses the technology of peer-to-peer (P2P) distributed ledger for various transactional applications [27], [28]. The decentralized attribute of this technology and publicly available data in blockchain network establish transparency and trust. Although, it is considered as the primitive component of cryptocurrencies but the technical framework including distributed network, shared ledger and digital online transactions are obvious to be used in any transactional process. We have described each of these components briefly in the following.

1) DISTRIBUTED NETWORK

Blockchain is depending upon a distributed network where each node has equal advantage without any priority or weightage or controlled by any other node. Therefore, blockchain networks are considered to be the part of extended peer-to-peer network design. Every node in the network stores a current or updated copy of the block chain and contributes to the cumulative method of verifying and certifying digital transactions or data access for the network.

2) DISTRIBUTED LEDGER

All the nodes in the network maintain a shared record of transactions known as ledger. This process makes the overall blockchaining as a trusted and transparent method of implementation. The nodes run algorithms to measure the validity of an initiated transaction of a digital record and verify the planned dealing. If a majority of the nodes within the network agrees about the validity of the transaction, then the

new transaction of the digital data is included in the block chain, recorded in the ledger and broadcast in the network for update. As the update decision is a group decision, therefore any node will not be able to tamper the record or ledger data at any point of time and therefore the openness of the process eventually provides the integrity of the shared ledger.

3) DIGITAL TRANSACTIONS

There is no data quality or syntax limitation in such technology, but a predefined data type needs to be agreed upon decision while implementing such application-specific blockchain. Data is encrypted and digitally signed to ensure legitimacy and accuracy. Transactions are structured into blocks and every block contains a cryptographic hash to the previous block within the block chain.

4) CONSENSUS

Consensus protocols are one of the important and unique features of blockchain technology. These protocols create a system that is not able to disapprove of an agreement as the protocols are being executed with a common agreed upon decision. It also helps in preventing exploitation of the system. Blockchain consensus protocols help all the nodes on a blockchain network to be synchronized with each other with a single overall decision at a time. Various consensus approaches exist including Proof-of-work, Proof-of concepts, Smart contracts, Consensus without mining, Tendermint consensus etc. [29], [30].

B. RECENT APPLICATION DEVELOPMENTS IN BLOCKCHAIN TECHNOLOGY

A blockchain based privacy preserving system for workers' location has been shown recently [31]. The framework uses a rewards-based task assignment process and anonymity features of blockchain to hide the identity information of users. Privacy ensured platforms for e-healthcare systems on blockchain environment have been a current topic of research in this direction [32], [33]. One research work uses Elliptic Curve Cryptography (ECC) to provide the security services to the healthcare management and provides anonymity to the health data. The another one provides access control and interoperability using smart contracts and advanced cryptographic primitives. A machine learning based privacy framework for blockchain has been identified recently [34]. It uses fair data trading protocol in big data market and implements its privacy-security features with ring signature, double-authentication-preventing signature and similarity learning. Solidity smart contract has been integrated to achieve the consensus. A privacy providing blockchain framework for transaction processing system has been designed for real time accounting, fraud monitoring and detection [35]. Another privacy preserving approach is shown in [36]. It integrates the power of blockchains with trust to solve the problems of traditional blockchain architectures. Apart from the above-mentioned recent developments with explicit privacy preservation, some generic applications of blockchain technology have been researched that provides the basic level of privacy of data by implementing cryptographic measures. These applications range from cyber security to enterprise systems though do not limit to the specific application with its abundance scope of feasibility in all spheres of present technology [37]–[45].

Smart contract developments in blockchain is another part of blockchain research which is significant to mention [46], [47]. Smart contracts are digital contracts executed in blockchain framework. As blockchain is using security measures, security techniques need not to be executed for smart contracts explicitly. Smart contracts have been researched for energy systems recently [48], [49]. Distributed renewable energy systems with heterogeneity and demand flexibility has been addressed here. Smart contracts have also been proved feasible for tracking articles in supply chain management. Business Process Re-engineering (BPR) across enterprise borders has been implemented by the work. Smart contracts are also implementable in banking systems that improves the financial loan management [50]. The authors have used permissioned blockchain Hyperledger Fabric for the purpose.

The above discussed developments in the field of blockchain gives an obvious impression that blockchain has spread its wings in various applications of our present technology. However, its applicability in human resource management in global platform has not been researched yet. Therefore, we have tried to implement the smart contracts in blockchain in human resource management.

III. PROPOSED SYSTEM

The distributed transparency and decentralized features have motivated us for this present work. We have proposed a blockchain based model through which human resource records can be created and verified on a distributed global platform which would help for reducing the job fraudulent on both employee and employer perspective. The overall proposed model is shown in Figure 1.

A. SYSTEM MODEL

Multiple organizations can take part simultaneously in the HRR blockchain. They should have a wallet which is a combination of some attributes such as IDs and cryptographic keys. This wallet is important for both storing the data and accessing the data in and out of the HRR distributed ledger. Any query for storing and accessing must be validated with proper wallet attributes and accordingly either to be granted or rejected. The extended processes are shown in Figure 4. A new trust score called Organization Trust Score (OTS) has been introduced that defines a scoring scheme out of 10 for employees given by the organization for the employees. This will also help to ensure for other organization to trust the employee as well. The model is segregated in different modules that starts with data level classification as unclassified, classified, secret and top secret. The following attributes of HRR are used to maintain the data privacy level as shown

TABLE 1. Data privacy levels for HRR.

Privacy level 1	Unclassified	Email id	open access
Privacy level 2	Classified	Sex, Age, Ethnicity, Previous Experience, Educational qualifications and achievements, Organization Trust Score (OTS)	pseduo-identity
Privacy level 3	Secret	Salary, Financial documentation	unlinkability
Privacy level 4	Top Secret	Contact number, address, Sexual orientation	anonymity, pseduo-identity, unlinkability

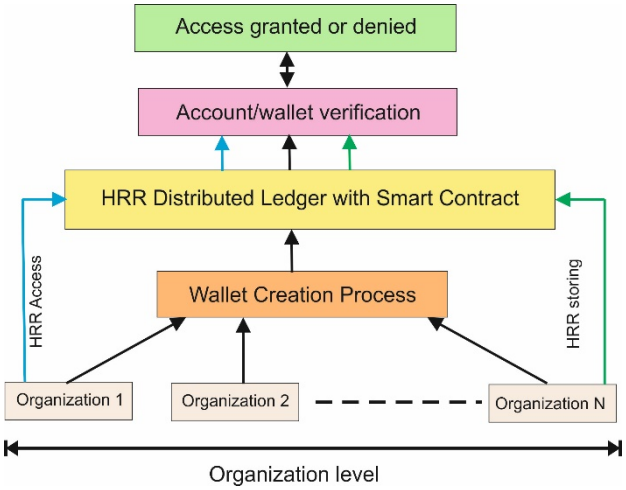


FIGURE 1. Proposed blockchain based HRR management model.

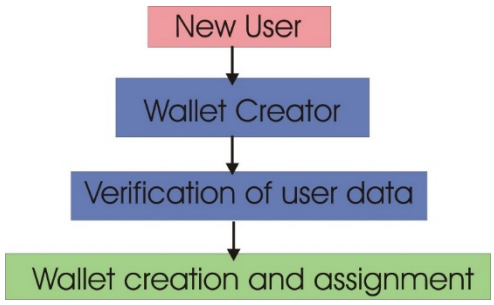


FIGURE 2. Steps for wallet assignment.

in Table 1. In the proposed system model, we have considered each organization that are willing to access any Human Resource Record (HRR) need to be registered with the blockchain network. Once they are registered, they need to apply for account assignment process as in Figure 2. This account assignment process is nothing but a generation of public-private key combination so that each organization can use those keys as per the cryptographic applications' requirements for creating or verifying an HRR block. Moreover, each account has been considered to have a wallet id (W_{ID}) to identify the corresponding organization. Therefore, as per the model, the wallet consists: $[W_{ID}, ID_{org}, Org_{pr}, Org_{pu}]$ where W_{ID} is the wallet ID and mapped with organization id ID_{org}. ID_{org} is mapped with wallet id W_{ID} by applying SHA-512 cryptographic hash on the ID_{org} and then taking M bits randomly using symmetric function generator and timestamp. This mapping provides pseudo-identitity of the organization identity and also helps in security services. After the mapping is done, RSA key generation is executed for public-private key pairs [62] at the gateway servers of the blockchain. For this process, W_{ID} and Symmetric Random Function Generator is used for selection of RSA parameters [63]. RSA outputs public-private key pair (Org_{pr}, Org_{pu}) for each W_{ID} which is stored by the key server. The key server has been considered to be secure and trusted. Thus, the wallet quad elements are generated as: $\{ID_{org}, W_{ID}, Org_{pr}, Org_{pu}\}$. These keys are generated by the trusted blockchain key servers which is responsible for distributing keys secretly.

Any HRR query Q is encrypted with Org_{pr} which further hashed with SHA-512. This provides digital signature. The hashed output of encrypted $SHA512[[Q]Org_{pr}]$ is then concatenated with 64 bits timestamp and then encrypted with Org_{pu} and sent for blockchain transaction. SHA-512 hashing provides integrity and using of Org_{pu} provides confidentiality. As a result, the message that pass through in blockchain network is in format of: $[SHA512[[Q]Org_{pr}||timestamp]]Org_{pu}$. In our experimentation, SHA-512 is of 512 bit hash, random number generator works with 512 bit configuration, public-private key bits are of 256 bits each and time stamp is of 128 bits. The overall process of HRR request execution is shown in Figure 4 which is extended from Figure 1. The theoretical steps are given below.

Step 1: A user (any organization who wants the HRR) joins the HRR Distributed Ledger in the blockchain network by providing the digital signature and request for an HRR.

Step 2: Once the request has been made and authentication has been proved, the user executes a smart contract system and waits for the conditional verdict.

Step 3: Once smart contract is over, the requested transaction has been validated and the record is added in the ledger in encrypted format as reencryption.

Step 4: All the members in the block chain network update their own ledgers accordingly and broadcast in the network.

The overall process is summarized in Algorithm 1. The proposed blockchain solution is to be applied in edge computing layer as the devices in this layer are suitable resource enabled to support blockchain applications. The storage for this application can be used in two ways, either a public cloud

Algorithm 1 HRR Query Processing

1: **Input:** ID_{org},HRR query Q
2: **Output:** HRR access
3: while ($i! = 0$)
$\{W_{ID}^{i} \leftarrow SRFG[SHA512(ID_{org})||timestamp]$, i is the index of organizations
$RSA_{key(W_{ID}^{i}, SRFG(W_{ID}^{i}))}$ { return (Org_{pr}, Org_{pu}) for every each $W_{ID}^{i}\}$
Create wallet:$\{ID_{org}, W_{ID}, Org_{pr}, Org_{pu}\}$
} end while
4: Organization → HRR blockchain: $SHA512([Q]_{Org_{pr}})_{Org_{pu}}$
5: Verification of signature and integrity in blockchain
6: Data parsing for privacy classification with Python
7: Execute smartcontract1( )
8: return access with reencryption to the valid user;
9: Commit transaction

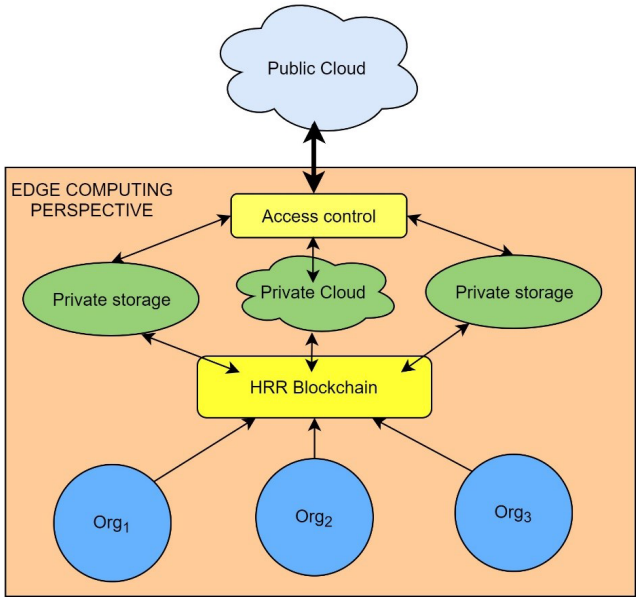


FIGURE 3. Edge-cloud computing perspective in HRR blockchain.

and each organization are having private cloud and can be connected with public cloud with access control mechanism and blockchain attributes. The relation between the proposed solution and the edge-cloud computing is shown in Figure 3. It shows that organizations are connected in the edge layer (perception layer). HRR blockchain is made by the organizations which then control the storage and access control. Depnding on the requirement of an organization, it can be private cloud or public cloud where the blockchain data is to be stored. However, for better generalization it should be connected with public blockchain with some specific data view.

B. SMART CONTRACT IN HRR DISTRIBUTED LEDGER

A smart contract is an executable program that is executed to mediate contractual interactions between two or more parties [46]. In this present work, the organizations are considered to execute the smart contract depending upon the data one organization is trying to access. The access of HRR is based on the data privacy levels and the conditions of the smart contracts have been programmed with these privacy levels only. It helps to avoid any further negotiation on the transparency of the data available in the HRR blockchain. This privacy level based smart contract also helps to ensure the privacy protection in the blockchain as the access conditions are open to everyone. The smart contract logical expression used in the present work has been shown as follows.

SmartContract1()
if HRR contains Data privacy level 1
Accessgrant ();
Else if HRR belongs to (Data privacy level 2 *or Data privacy level 3)*
Accessgrant (check validation);
Else
Accessdeclined();

Smart contracts also help to detect deviations from the agreed upon behaviour among organizations. The declaration of the verdict is directly and intricately associated to an action (for example, accessing or storing of record) that is executed when the verdict is positive. Moreover, it provides reliability because smart contracts are stored in hash format and are accessible by the users only after verification of wallets. Therefore, any change in smart contract also need to be validated by the all blockchain participants. SHA-512 is used for this process. The blockchain itself executes this hashing process so that integrity and reliability can be maintained.

C. PRIVACY AND HRR VALIDITY CHECKER

In the proposed model shown in Figure 4, we have added a module of anonymity and HRR request validity checker. Once the smart contract is initiated, HRR request is parsed and data contains are classified as per the privacy levels. If a disjoint or malicious owner tries to access any illegitimated data level, access is denied further. Moreover, the use of digital signature with the wallet keys also provides the basic cryptographic services of confidentiality, integrity and digital signature which is very much important for a public infrastructure like blockchain.

IV. FEASIBILITY OF BLOCK CHAIN MODEL IN HRR TRANSACTIONS

Any block chain for HRR management must be open and public without any hindrance to properly analyse the usage of the HRRs by the employers. Additionally, we have provided the feasibility of the proposed approach in terms of measurability and access privacy and also have shown the advantages in the following subsections.

A. MEASURABILITY

A distributed ledger in blockchain infrastructure contains the employee records with different data levels that have information storage implications and information output limitations.

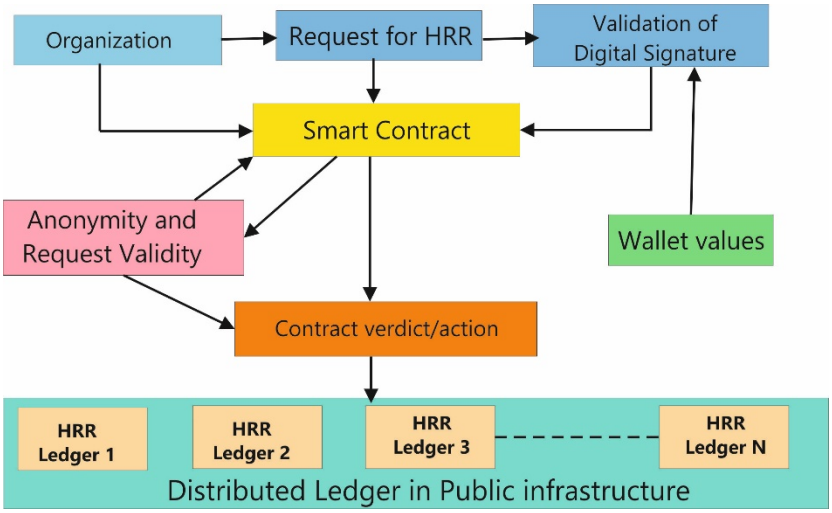


FIGURE 4. Schematic process for HRR distributed ledger access.

It is not possible that telephonically or manually you are verifying the newly joined employees in the organization where the process is oftem time consuming and non-technical and sometime biased. Therefore, we have developed the model in blockchain based HRR management model where distributed ledgers are used. Employees can be verified by the employers at any point of time just initiating the transaction and checking the OTS. The historical records of the employee and its experience and background therefore can be checked easily in the blockchain process where the chain of records of the employee provides a low cost technical and efficient solution for HRR management.

All HRR information are to be managed in an HRR pool. Various cryptographic processes specifically encryption decryption process can be used for the secured storage of this pool. In the presented work, we have used public key encryption to ease out the basic functionality of the proposed model. Three levels of HRR pool have been generated depending upon the parsed data in HRR. The requested HRR must be related with one of the categories or partially to all the categories. The pseudoidentity of the employees are enabled with the Anonymizer module which is shown in Figure 4. HRR pools are extendable and should store various types of information, from pictures to documents to key-value stores. The market researchers and human resource department of the employer may use the data of the employees as per the privacy policy. It also helps in predictive analysis of in the organization regarding the shift culture of the employees. Figure 5 represents a HRR pool showing the various components. Cryptographic processes, wallet verification and smart contract validation provide the reliability and the integrity of the HRR pool data.

B. ACCESS SECURITY AND INFORMATION PRIVACY

The blockchain is distributed and open, therefore the information access must include some security condition. The user who are sharing the information will have full access to its own information and management in what manner its information are to be shared. The permission of the information access is to be given after verifying the digital signature of the query requester.

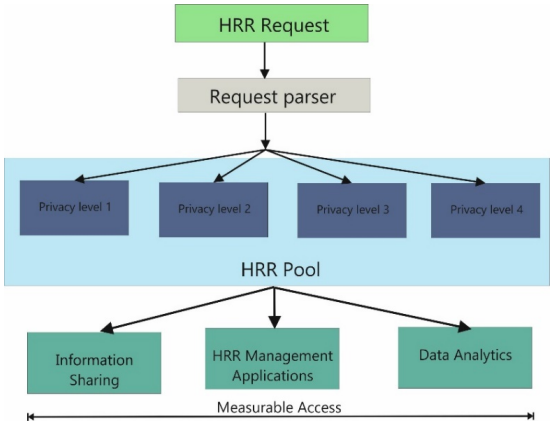


FIGURE 5. Proposed concept of HRR pool.

Access management permissions are versatile and are handled over "all-or-nothing" permissions depending smart contract conditions among the parties. The user would setup specific, elaborate transactions regarding which user has access, the assigned time-frame for access and therefore the specific forms of information which will be accessed. At any given time, the employer is to be allowed to alter the set of functions in smart contract. Access management policies are to be firmly kept on a blockchain. and solely the user would be allowed to vary them. This provides associate degree setting of transparency and permits the user to create all choices regarding what information is collected and the way the information is often shared. The use of digital signature and public key cryptography in the proposed model ensures the security services including confidentiality, integrity, digital signature, non-repudiation respectively [51]. The process is shown below in Figure 6. The use of SHA-512 for the

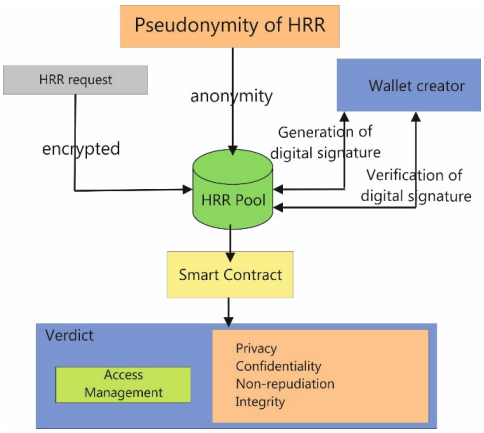


FIGURE 6. Access permission process.

encrypted query Q provides integrity to the query. RSA provides security for the key generation process. Diffie-Hellman Key Exchange algorithm for the process [52]. Data parsing helps to access only legitimate and shareable information from the documents and W_{ID} are used for anonymity. Therefore, the proposed system is efficient in maintaining security and privacy.

C. TECHNICAL BENEFITS OF HRR BLOCKCHAIN

Blockchain technology offers several benefits for various applications such as medication analysis, distributed diagnosis EMRs, emergency consultancy of group of doctors and obviously research purpose and identifying new symptoms or medicines for a health problem. It is also able to handle larger volumes of knowledge and a lot of blockchain users. The design has inbuilt fault tolerance and disaster recovery, and also the cryptography technologies for providing security services such as authentication and confidentiality are wide used and accepted as business standards. Therefore, we have attempted with the presented research problem in a blockchain model along with preserving the privacy of the users and the security of the data. Blockchain works with commonplace algorithms and protocols for cryptography and encryption. These technologies are heavily analysed and accepted as secure and are wide used across all industries and plenty of government agencies. The most advantageous part of this model includes:

- It is public and transparent and openly available with various data levels.
- Privacy levels can be altered by the data owner only and therefore smart contract can be changed with owner permission.
- The public key infrastructure provides the cryptographic security services to smart contract, legitimate access and secure HRR transactions.
- This infrastructureless blockchain technology would be a great and effective solution for managing human resource records worldwide; reducing the fraud activities applicable for employer and employee both.

The blockchain model in the proposed system itself provides the basic level of security and access control, whereas, connecting it IoT framework and cyber-physical systems, we can follow the process of location awareness concept as shown in [53], [54]. Further, the attributes of the HRRs can be analysed with deep learning methods for automatic process of privacy settings [55]. The blockchain is distributed and transparent and therefore the storage (i.e. the cloud storage) too plays an important role while deploying a model. Dynamic cloud resource management therefore must be taken into consideration while conjugating the proposed model with IoT backbone [56]–[58].

V. PERFORMANCE EVALUATION

In the present case, performances are measured in terms of memory consumption and processing speed (time). The implementation parameters are listed in Table 2. Due to the lack of works in human resource management application of blockchain and smart contracts, we have measured the present systems' performance only. The implementation process and related results are discussed in following subsections.

TABLE 2. Implementation metrics.

Consensus protocol	Solidity consensus (smart contract) [52]
Geographic distribution of nodes	Wide area network (WAN) environment, 50 nodes
Hardware environment of all peers	3.3 GHz, 16 GB RAM, Octa-core, 2 TB HDD
Network model	Campus Area network connected with a WAN with three routers and two firewalls
Number of nodes involved in the test transaction	6
Test tools and framework	Hyperledger Caliper
Type of data store used	CouchDB

A. IMPLEMENTATION PROCESS

We have used Ethereum network with solidity contract and Remix IDE for the compilation of the solidity. The detailed steps are as follows.

Step 1: Pre-installation of Homebrew and Node/npm.
Step 2: Installation of Ethereum, Solidity and Remix IDE.
Step 3: Genesis blocks are initialized.
Step 4: HRR chain is initialized with two blocks and three virtual organization accounts with wallets.
Step 5: A folder is created for the blockchain to reside.
Step 6: Private Ethereum Blockchain is initiated and run.
Step 7: Geth Javascript console is used to connect to the private Ethereum blockchain.
Step 8: Account has been created and dummy Ethers are mined.
Step 9: Smart contract condition is created in solidity and included in Ethereum.
Step 10: Remix IDE is initialized to deploy the generated smart contract.
Step 11: remix IDE is updated with wallet account of the organization and blockchain network details.

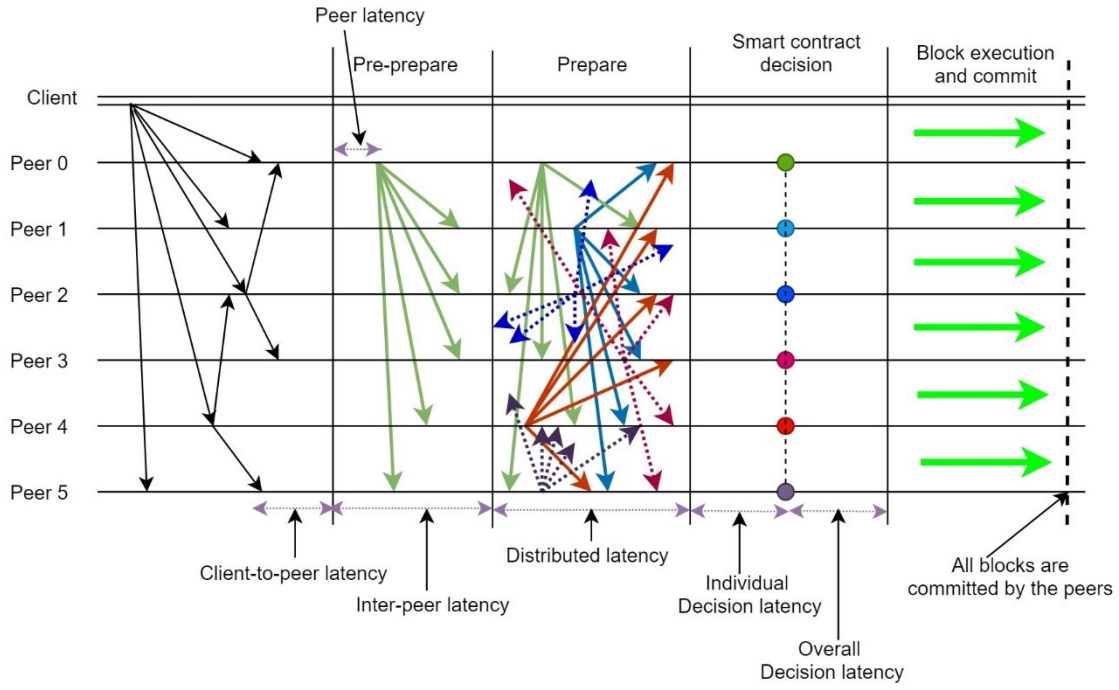


FIGURE 7. Transaction flow of HRR blocks commitment by testing peers.

Step 12: Smart contract is executed on Ethereum blockchain.

B. RESULTS

We have measured the systems performance to generate 50 HRRs blocks. The system commitment by all the peers of the HRR blockchain network has been shown by a transaction flow diagram as shown in Figure 7. The figure shows that the smart contract condition helps in simultaneous commitment of the transactions reaching to a unanimous decision for HRR block access which leads to the minimum latency as shown in Table-4 later. Six peers are used for the testing process and colour codes are represented for peer wise transaction. The coloured circles in the smart contract decision process represents the point of decision. As smart contract is executed on distributed platform, the decision point comes out is same for all the peers which is beneficial for using the model. The latencies observed here are categorized as client to peer latency, peer latency, distributed latency, individual and overall decision latency. Client-to-peer latency is defined as the time the access request is put by the client and the peers receives the request. Peer latency is the latency for individual peer whereas inter-peer latency calculates latency for all the peers and gives in an average value out of all peers. Distributed latency calculates the time for communicating the access request with all other peers. Individual decision latency is taken by individual peer to execute the smart contract decision and the overall decision latency is the time taken for the unanimous decision for the HRR access. Once decision is reached by all the peers, all the transactions are committed by the respective peers shown with green bolded arrows. All these latencies are involved in measuring the read latency and transaction latency. Read latency includes client to peer latency, peer latency, and distributed latency. Transactional latency includes read latency and individual and overall decision latency.

TABLE 3. Commit time of node(s).

Node No.	Node 1	Node 2	Node 3	Node 4	Node 5	Node 6
Commit time (seconds)	1.33	2.40	1.33	1.77	2.74	1.47

We have measured the commit time of six nodes participated in the test process of the model and the measurements are given in Table-4. The commit times help in calculating the Transactional latency and transactional throughput. Measurement of latency time and memory consumption is important for blockchain based application because in a real-life environment low latency and less memory are desirable factors for blockchain based applications. Four different types of timing are measured here: time for parsing HRRs, read latency for a single block of HRR, transaction latency and time for a smart contract verdict. For the second and third metric measurement, we have followed the metric definition and calculation process as shown in [61]. We have used Javacc for the parsing process. Memory consumption is also measured to check whether the proposed system is creating a memory overload problem.

From the Table 4, it is observed that with increasing number of HRR blocks the timing parameters increase lin-

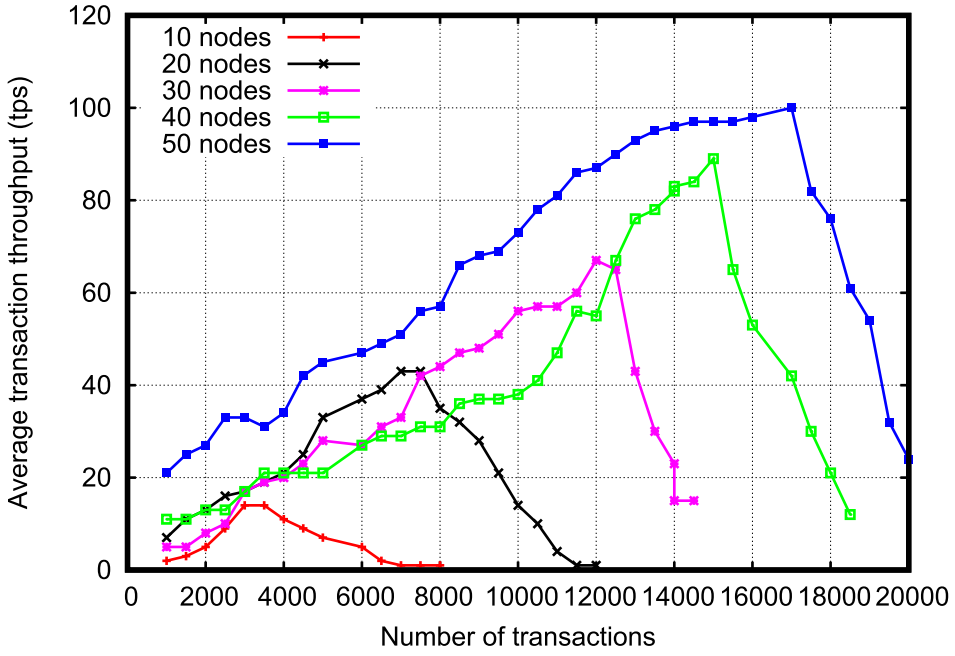


FIGURE 8. Concurrent transaction capacity with varied number of nodes.

TABLE 4. Proposed approach performance.

Performance Metrics	Number of HRRs					
	10	20	30	40	50	Measured complexity
Time consumption for parsing HRRs (seconds)	11.23	23.33	34.77	45.33	56.73	o(n)
Read latency as time between read request of HRR and access of HRR for a single block of HRR	4.66	5.5	7.33	9.01	9.35	o(n)
Time consumption for overall access of HRR called as Transaction latency (seconds)	23.43	37.70	51.33	65.21	74.23	o(nlogn)
Time consumption for Smart Contract process (seconds)	2.33	3.05	3.77	5.66	6.33	o(Nlogm)
Memory consumption (KB)	91	173	262	342	428	o(n)

early giving a stability to the system. The measured complexities of the proposed approach are almost linear and therefore it is efficient in blockchain application paradigm. We have also performed the analysis on Hyperledger Caliper framework [61] to test the proposed blockchain solution. The results are observed as in Table 5 the measurement for some important parameters as per the Caliper framework. The experimental results depict that with the increasing total number of blocks from 10 to 50 the average delay also increases with by 2 %. It signifies that the proposed system is quite stable in delay and therefore jitter is less which is advantageous for real life applications. Moreover, the throughput has been measured in transactions per second (tps) which is almost linear. In the experimentation, we have considered the transactions as complete block of HRR access. We have tested the system model to determine the capacity

TABLE 5. Results for Caliper framework.

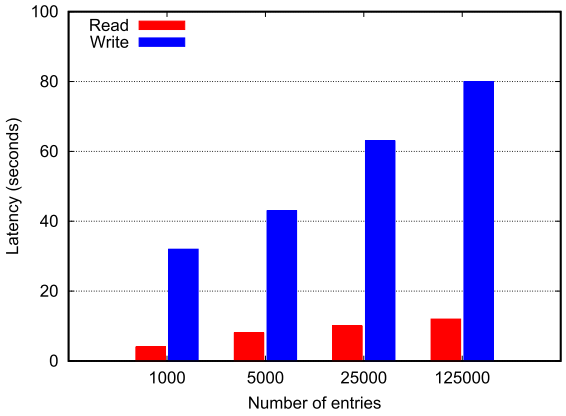
Blocks of HRR	Success rate	Maximum delay (seconds)	Minimum delay (seconds)	Average delay (seconds)	Transaction Throughput
10	100%	23	11	17	2 blocks/sec
20	100%	31	14	22.5	4 blocks/sec
30	100%	43	21	32	7 blocks/sec
40	100%	48	21	34.5	11 blocks/sec
50	100%	52	32	42	14 blocks/sec

of concurrent transactions handling. The number of nodes is varied from 10 to 50 and concurrent transactions are started from 1000 transactions until the failure point has been observed. The condition of the failure has been fixed as the transaction latency is greater than 15 minutes. The failure points or the system capacity is shown in Figure 8 and also given in Table 6.

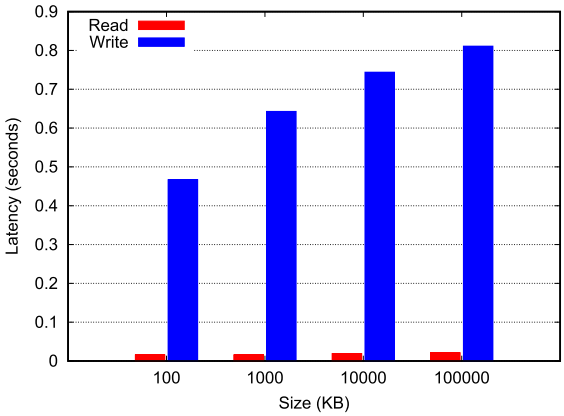
TABLE 6. Failure point observation.

Number of nodes	Number of Concurrent transactions capacity	Average Transaction throughput (tps)	Overall commit time of all the transactions (min)
10	3500	17	10.33
20	8000	43	27.67
30	12000	58	37.02
40	15000	85	46.33
50	17000	100	51.90

The above table shows the concurrent transaction capacity that signifies the fact with the increasing number of nodes, concurrent transaction handling capacity increases by ≈ 1.6 times. Similar proportion of increase in throughput of transactions is also observed with average increase of $\approx$ 1.37 times notifying 60.6 tps on average for all



(a) Number of entries in blockchain



(b) Size of the blocks

FIGURE 9. Results of micro-benchmarking experiments for read-write operations.

the transactions. The in-depth observation of the transactions and capacity is shown in Figure 8. Figure 8 depicts the behaviour of the proposed system with the increasing number of transactional peers (nodes) and increasing number of transactions. The transaction throughput in case of 10 nodes has been observed to increase upto 3500 concurrent transactions with average throughput of 17 tps. The throughput increases by 0.23% for each 500 transaction, however, after 3500 transactions the performance starts degrading and becomes almost zero with 8000 transactions. Similarly, the observation for 20 nodes, 30 nodes, 40 nodes and 50 nodes are noted as increasing factors for throughput are 0.3%, 0.47%, 0.5% and 0.76% respectively. The average throughputs for the 10 node, 20 node, 30 node, 40 node and 50 node scenarios are resulted with 43, 58, 85 and 100 tps on average respectively. We have followed the two micro benchmarking experiments to measure the latency of the system by varying the number of read-writes performed by the transactions [54]. We have used different sized key-value stores and transactions with variable event payloads. Transaction latencies are recorded on average for a large number of transactions with a single client to submit transactions and a single peer for admitting it. In the first experiment, the number of key-values read (read-set) and the number of key-values written (write-set) is varied with the objective to understand the effect of the increasing number of the read-set and the write-set on transaction latency. Similarly, size of the smart contract key value is another parameter to measure the effect of read-write latency. We have experimented this with increasing the size of smart contract key. The results are shown in Figure 9a and Figure 9b respectively.

Figure 9 shows that the write latency increases with increasing number of transactions by 3.4% in each variation of increased size. Read latency, however, is stable as compared to write latency. Similarly, the smart contract key size increases from 100 KB to 100000 KB with write latency increased by 50% and read latency by 0.15%. These latencies essentially signify that if the read-write latency degrades with the size of the key-value store but increases significantly over time due to a greater number of transaction entries. Finally, we have theoretically compared the presented work with the generic (manual) HRR management process and the comparison is summarized in Table 7. The properties compared in the Table 5 show that the proposed approach is efficient in handling human resource records in global platform.

TABLE 7. Comparison of features.

Features of comparison	Generic HRR management	Proposed Blockchain based HRR management
Platform of Operation	Local	Global
Transparency	No	Yes
Traceability	No	Yes
Privacy	No	Yes
Confidentiality and Digital structure	Explicit requirement	Implicit with blockchain
Consensus	No	Yes (smart contract)
Anonymity	No	Pseudo-anonymity
Privacy levels consideration	No	Yes (4 levels)
Time consuming	more	less
Memory consumption	Non-linear	linear
Digital forensics	Ambiguous and biased	Non-ambiguous, transparent and easy
Distributed	No	Yes
Fault Tolerant	No	Yes

C. SECURITY AND PRIVACY ANALYSIS

Claim 1: The proposed HRR blockchain model is secure against tampering of data by an adversary.

Threat Model: The HRR blockchain contains records of employee credentials. The adversary aims to either modifying some data or replace the original data with the new one.

Argument: The uploaded HRR data is encrypted as $SHA512([Q]_{Org_{pr}})_{Org_{pu}}$ and stored on a cloud server. The link to these encrypted HRRs is known only by the gateway server. The adversary cannot modify the real encrypted HRR data as it needs key. The combination of public-private key is generated with the help of wallet id and random number.

Therefore, breaking this combination requires to know exact random number used for generation of the key pairs which infeasible in the present computing technologies as Symmetric Random Function generator (as used here) possesses properties of true random number. Even though in the worst case, if the attacker is able to modify or replace the any encrypted HRR data, the message digest on the blockchain ensures the detection. If the adversary wants to modify the metadata on the blockchain, an extensive work is required to construct a new main chain and have to be the part of smart contract.

Claim 2: The proposed HRR model is secure against a collusion between the gateway server and the adversary. *Threat Model:* Use of re-encryption keys or stale keys stored at the gateway server and collusive attempt to obtain the HRR data or re-encrypt the HRR data for the adversary.

Argument: As per generic blockchain application framework, access control list is locally stored at the gateway server which does not include any secret key. The gateway server, therefore, is unable to have access to the encrypted HRR data. Since, the private key is in the account of the HRR owner, i.e., the organization, the re-encryption keys used by the gateway server can only be generated by the HRR owner.

Claim 3: The proposed HRR model is secure against replay attack. *Threat model:* The adversary may copy a transaction of an authorized user from blockchain or by the way of intercepting the messages sent by an authorized user and then replay the message on the gateway server in order to obtain the HRR data.

Argument: The gateway server of the blockchain verifies time stamp along with the sender's signature If the timestamp is not found invalid or stale, the gateway server does not respond to the request. If the timestamp is still valid, the adversary will be able to obtain the reencrypted HRR; however, the adversary still cannot decrypt it due to the lack of the corresponding private keys.

Claim 4: The proposed HRR model is secure against malicious access.

Threat Model: A malicious user wants to read/write the HRR data without an authorization.

Argument: The signature process verifies an authenticated user. Besides, in the worst case, if signature is replayed or disguised, reencryption process will help to maintain confidentiality as the adversaries will not have the appropriate private keys.

Claim 5: The proposed HRR model is secure against key based attacks.

Threat Model: The attacker gets an intermediate data such as organization ID and predicts key combination for data access.

Argument: To generate the key pairs, organization ID is used with random function generator for selecting M bits which is randomly chosen in the SHA-512 output of the organization ID. Furthermore, RSA also uses random function for initialization and this wallet ID for key generation. Therefore, the probability of two keys are same has been given as:

$$P(k_1 = k_2) = \frac{1}{C_1{}^n_r.C_2{}^n_r.t} \approx 0$$

where, $C_1{}^n{}_r$ is the combination of possible IDs and $C_2{}^n{}_r$ is the combination of SRFG outputs with n = 512 and r = 256 bits, t is the timestamp bits.

Claim: The proposed HRR model preserves privacy. *Threat Model:* HRR consists of various data related to financial credentials and personal data. Data privacy breach can be done by the adversary by bypassing the access controls or privacy classification. *Argument:* The HRR model uses smart contract for maintaining access control properly. Privacy level classification is done. Ach classification is associated with privacy parameter as an objective. In privacy level 1 email-ids has been made open access and does not require any privacy concern. Though, phishing can be concern but we are not dealing with this in this present work. In privacy level 2, anonymity and pseudo anonymity are provided by SHA-512. The information about education, previous employment, OTS scores will not directly be visible as like an open access and therefore needs authentication by the requester. Salary and financial documentation like income tax in privacy level 3 will be under control of the blockchain owner so that unlinkability can be maintained and finally in privacy level 4, anonymity, pseduo-identity, unlinkability to be maintined by encrypting the information by the block owner.

VI. CONCLUSION

Blockchain technology is the future of digital world for providing security, transparency and distributed fault-tolerant behaviour. Every domain of the present technology has embraced the conjugation of blockchain with various extensions and updates. Human resource management is always a crucial part of any organization where the business functionalities depend upon human resource of that organization as the technical expertise and managerial aspects are evolved around them. Organizations face various reputation-based disadvantages from the human resource due to lack of synchronized verification of employee details. As a result, organizations working environment and their reputation may face a stake even with its various stakeholders. Therefore, we have come up with the solution of blockchain based framework with smart contracts that has been proved beneficial for managing human resource records in a transparent global and distributed platform. In the process, we have also maintained the privacy of the records depending upon its visibility and sharable features. The experimental results and the comparison between generic (manual) process and our proposed approach prove that the presented work is efficient. In future, we shall work on commit time optimization and optimizing the systems' performance by increasing the tolerance of the failure point with more number of concurrent transactions. We shall also try to explore the feasibility of attribute based encryption and homomorphic encryption for

re-encryption procedure for the observation of latency related system behaviour.

AUTHOR CONTRIBUTIONS

T.H. Kim and G. Kumar conceived the idea, designed the experiments and analyzed the data; M.Alazab studied the feasibility; M. K. Rai and R. Saha performed the experiments and conducted the analysis; R.Saha, G. Kumar and Y. Yin analysed the methods, interpreted the results and drew the conclusions; R. Saha and R. Thomas proof read the paper. All the authors agree with the above contribution details.

ACKNOWLEDGEMENT

(Tai-Hoon Kim and Rahul Saha contributed equally to this work.)

CONFLICTS OF INTEREST

All authors declare no conflict of interest.

REFERENCES

[1] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Mar. 20, 2019. [Online]. Available: https://www.bitcoin.org
[2] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.
[3] D. Efanov and P. Roschin, "The all-pervasiveness of the blockchain technology," *Procedia Comput. Sci.*, vol. 123, pp. 116–121, Jan. 2018.
[4] S. Meunier, "Blockchain 101: What is blockchain and how does this revolutionary technology work?" in *Transforming Climate Finance and Green Investment With Blockchains*, A. Marke, Ed. New York, NY, USA: Academic, 2018, pp. 23–34.
[5] S. Mansfield-Devine, "Beyond bitcoin: Using blockchain technology to provide assurance in the commercial world," *Comput. Fraud Secur.*, vol. 2017, no. 5, pp. 14–18, 2017.
[6] H. Gao, C. Liu, Y. Li, and X. Yang, "V2VR: Reliable hybrid-network-oriented V2V data transmission and routing considering RSUs and connectivity probability," *IEEE Trans. Intell. Transp. Syst.*, early access, Apr. 13, 2020, doi: 10.1109/TITS.2020.2983835.
[7] H. Gao *et al.*, "Transformation-based processing of typed resources for multimedia sources in the IoT environment," *Wireless Netw.*, 2019, doi: 10.1007/s11276-019-02200-6.
[8] Y. Acikgoz, "Employee recruitment and job search: Towards a multi-level integration," *Hum. Resource Manage. Rev.*, vol. 29, no. 1, pp. 1–13, Mar. 2019.
[9] Businesstopia in Human Resource. (Mar. 22, 2019). *Selection and Hiring Process*. [Online]. Available: https://www.businesstopia.net/human-resource/selection-hiring-process
[10] P. Vardarlıer, Y. Vural, and S. Birgün, "Modelling of the strategic recruitment process by axiomatic design principles," *Procedia-Social Behav. Sci.*, vol. 150, pp. 374–383, Sep. 2014.
[11] H.-S. Shih, L.-C. Huang, and H.-J. Shyur, "Recruitment and selection processes through an effective GDSS," *Comput. Math. Appl.*, vol. 50, nos. 10–12, pp. 1543–1558, Nov. 2005.
[12] A. J. Doherty, "Managing our human resources: A review of organisational behaviour in sport," *Sport Manage. Rev.*, vol. 1, no. 1, pp. 1–24, Nov. 1998.
[13] M. Diaz-Fernandez, S. Pasamar-Reyes, and R. Valle-Cabrera, "Human capital and human resource management to achieve ambidextrous learning: A structural perspective," *BRQ Bus. Res. Quart.*, vol. 20, no. 1, pp. 63–77, Jan. 2017.
[14] P. Boxall, J. Purcell, and M. P. Wright, *Human Resource Management: Scope, Analysis, and Significance*, 1st ed. New York, NY, USA: Oxford, 2008.
[15] W. T. York and D. MacAlister, "Human resources and staff responsibilities," in *Hospital and Healthcare Security*, W. T. York and D. MacAlister, Ed., 6th ed. Oxford, U.K.: Butterworth-Heinemann, 2015, pp. 359–378.
[16] D. Watson and A. Jones, "Human resources," in *Digital Forensics Processing and Procedures*, D. Watson and A. Jones, Ed. Rockland, MA, USA: Syngress, 2013, pp. 741–793.
[17] T. Rasmussen and D. Ulrich, "Learning from practice: How HR analytics avoids being a management fad," *Org. Dyn.*, vol. 44, no. 3, pp. 236–242, Jul. 2015.
[18] Q. Feng, J. Jaussaud, and X. Liu, "State-owned versus private enterprises in China: Adoption of modern HRM practices," in *The Globalization of Chinese Business* (Chandos Asian Studies Series), R. Taylor, Ed. Colchester, U.K.: Chandos Publishing, 2014, pp. 51–68.
[19] M. Laurent and C. Levallois-Barth, "Privacy management and protection of personal data," in *Digital Identity Management*, M. Laurent and S. Bouzefrane, Ed. Amsterdam, The Netherlands: Elsevier, 2015, pp. 137–205.
[20] (Mar. 23, 2019). *Safeguards for Domain 5 Information Security & Privacy Program*. [Online]. Available: https://protect.iu.edu/online-safety/program/safeguards/human-resources.html
[21] (Mar. 23, 2019). *What Do Human Resources Managers Need to Know About HIPAA Laws?* [Online]. Available: https://www.humanresourcesmba.net/faq/what-do-human-resources-managers-need-to-know-about-hipaa-laws/
[22] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3628–3636, Aug. 2018.
[23] J. Yu, Z. Kuang, B. Zhang, W. Zhang, D. Lin, and J. Fan, "Leveraging content sensitiveness and user trustworthiness to recommend fine-grained privacy settings for social image sharing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1317–1332, May 2018.
[24] J. Yu, B. Zhang, Z. Kuang, D. Lin, and J. Fan, "IPrivacy: Image privacy protection by identifying sensitive objects via deep multi-task learning," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1005–1016, May 2017.
[25] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, "Data security and privacy in cloud computing," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 7, pp. 1–9, 2014.
[26] O. Awodele, O. Akpovi, A. O. Adebayo, O. O. Tayo, "Security and privacy issues in cloud computing," *Commun. Appl. Electron.*, vol. 7, no. 3, pp. 14–17, 2017.
[27] (Mar. 30, 2019). *Blockchain Fundamentals: How Does It Actually Work?* [Online]. Available: https://dzone.com/articles/blockchain-fundamentals-how-does-it-actually-work
[28] D. Drescher, *Blockchain Basics*, 1st ed. New York, NY, USA: Apress, 2017.
[29] (Apr. 2, 2019). *Consensus*. [Online]. Available: https://mastanbtc.github.io/blockchainnotes/consensustypes/
[30] G. Kumar, R. Saha, M. K. Rai, R. Thomas, and T.-H. Kim, "Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6835–6842, Aug. 2019.
[31] M. Yang, T. Zhu, K. Liang, W. Zhou, and H. R. Deng, "A blockchain-based location privacy-preserving crowdsensing system," *Future Gener. Comput. Syst.*, vol. 94, pp. 408–418, May 2019.
[32] A. A. Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Gener. Comput. Syst.*, vol. 95, pp. 511–521, Jun. 2019.
[33] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, pp. 283–297, May 2018.
[34] Y. Zhao, Y. Yu, Y. Li, G. Han, and X. Du, "Machine learning based privacy-preserving fair data trading in big data market," *Inf. Sci.*, vol. 478, pp. 449–460, Apr. 2019.
[35] Y. Wang and A. Kogan, "Designing confidentiality-preserving blockchain-based transaction processing systems," *Int. J. Accounting Inf. Syst.*, vol. 30, pp. 1–18, Sep. 2018.
[36] U. Jayasinghe, G. M. Lee, Á. MacDermott, and W. S. Rhee, "TrustChain: A privacy preserving blockchain with edge computing," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–17, Jul. 2019.
[37] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Informat.*, vol. 36, pp. 55–81, Mar. 2019.
[38] L. Axon, M. Goldsmith, and S. Creese, "Privacy requirements in cybersecurity applications of blockchain," in *Advances in Computers*, vol. 111, P. Raj and G. C. Deka, Ed. Amsterdam, The Netherlands: Elsevier, 2018, pp. 229–278.

[39] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for Internet of Things," *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019.

[40] X. Pan, X. Pan, M. Song, B. Ai, and Y. Ming, "Blockchain technology and enterprise operational capabilities: An empirical test," *Int. J. Inf. Manage.*, vol. 52, Jun. 2020, Art. no. 101946.

[41] Y. Wang, M. Singgih, J. Wang, and M. Rit, "Making sense of blockchain technology: How will it transform supply chains?" *Int. J. Prod. Econ.*, vol. 211, pp. 221–236, May 2019.

[42] 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, Jan. 2018.

[43] J. Chen, Z. Lv, and H. Song, "Design of personnel big data management system based on blockchain," *Future Gener. Comput. Syst.*, vol. 101, pp. 1122–1129, Dec. 2019.

[44] Y. Jin, X. Guo, Y. Li, J. Xing, and H. Tian, "Towards stabilizing facial landmark detection and tracking via hierarchical filtering: A new method," *J. Franklin Inst.*, vol. 357, pp. 3019–3037, Mar. 2020, doi: 10.1016/j.jfranklin.2019.12.043.

[45] Y. Yin, F. Yu, Y. Xu, L. Yu, and J. Mu, "Network location-aware service recommendation with random walk in cyber-physical systems," *Sensors*, vol. 17, no. 9, p. 2059, Sep. 2017.

[46] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study," *Telematics Informat.*, vol. 35, no. 8, pp. 2337–2354, Dec. 2018.

[47] X. Liu, K. Muhammad, J. Lloret, Y.-W. Chen, and S.-M. Yuan, "Elastic and cost-effective data carrier architecture for smart contract in blockchain," *Future Gener. Comput. Syst.*, vol. 100, pp. 590–599, Nov. 2019.

[48] Y. Li, W. Yang, P. He, C. Chen, and X. Wang, "Design and management of a distributed hybrid energy system through smart contract and blockchain," *Appl. Energy*, vol. 248, pp. 390–405, Aug. 2019.

[49] X. Wang, W. Yang, S. Noor, C. Chen, M. Guo, and K. H. van Dam, "Blockchain-based smart contract for energy demand management," *Energy Procedia*, vol. 158, pp. 2719–2724, Feb. 2019.

[50] H. Wang, C. Guo, and S. Cheng, "LoC—A new financial loan management system based on smart contracts," *Future Gener. Comput. Syst.*, vol. 100, pp. 648–655, Nov. 2019.

[51] L. Wang, X. Shen, J. Li, J. Shao, and Y. Yang, "Cryptographic primitives in blockchains," *J. Netw. Comput. Appl.*, vol. 127, pp. 43–58, Feb. 2019.

[52] W. Diffie and E. M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[53] H. Gao, Y. Xu, Y. Yin, W. Zhang, R. Li, and X. Wang, "Context-aware QoS prediction with neural collaborative filtering for Internet-of-Things services," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4532–4542, May 2020, doi: 10.1109/JIOT.2019.2956827.

[54] Y. Yin, W. Zhang, Y. Xu, H. Zhang, Z. Mai, and L. Yu, "QoS prediction for mobile edge service recommendation with auto-encoder," *IEEE Access*, vol. 7, pp. 62312–62324, 2019.

[55] R. Yang, J. Zhang, J. Wan, L. Zhou, J. Shen, Y. Zhang, Z. Wei, J. Zhang, and J. Wang, "Parameter communication consistency model for large-scale security monitoring based on mobile computing," *IEEE Access*, vol. 7, pp. 171884–171897, 2019.

[56] J. Yu, J. Li, Z. Yu, and Q. Huang, "Multimodal transformer with multi-view visual representation for image captioning," *IEEE Trans. Circuits Syst. Video Technol.*, early access, Oct. 15, 2019, doi: 10.1109/TCSVT.2019.2947482.

[57] J. Yu, M. Tan, H. Zhang, D. Tao, and Y. Rui, "Hierarchical deep click feature prediction for fine-grained image recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, early access, Jul. 30, 2019, doi: 10.1109/TPAMI.2019.2932058.

[58] J. Yu, C. Zhu, J. Zhang, Q. Huang, and D. Tao, "Spatial pyramid-enhanced NetVLAD with weighted triplet loss for place recognition," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 2, pp. 661–674, Feb. 2020, doi: 10.1109/TNNLS.2019.2908982.

[59] (Apr. 12, 2019). *Smart Contracts*. [Online]. Available: https://solidity.readthedocs.io/en/v0.4.24/introduction-to-smart-contracts.html

[60] (Apr. 15, 2019). *Hyperledger Caliper*. [Online]. Available: https://www.hyperledger.org/projects/caliper

[61] *Hyperledger Performance and Scale Working Group, Hyperledger Blockchain Performance Metrics*. Accessed: Apr. 10, 2019. [Online]. Available: https://wiki.hyperledger.org/groups/pswg/performance-and-scale-wg

[62] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[63] R. Saha and G. Geetha, "Symmetric random function generator (SRFG): A novel cryptographic primitive for designing fast and robust algorithms," *Chaos, Solitons Fractals*, vol. 104, pp. 371–377, Nov. 2017.

TAI-HOON KIM (Member, IEEE) received the B.E. and M.E. degrees from Sungkyunkwan University, South Korea, and the Ph.D. degree from the University of Bristol, U.K., and the University of Tasmania, Australia. His main research interests include security engineering for IT products, IT systems, development processes, and operational environments.

GULSHAN KUMAR received the B.Tech. degree in computer science engineering from the Amritsar College of Engineering, Amritsar, in 2009, and the M.Tech. and Ph.D. degrees from Lovely Professional University, Punjab, India, with area of specialization in position and location computation in wireless sensor networks. He is currently working as an Associate Professor with Lovely Professional University. He has many publications in well renowned International journals and Conferences.

RAHUL SAHA received the B.Tech. degree in computer science engineering from the Academy of Technology, West Bengal, and the M.Tech. and Ph.D. degrees from Lovely Professional University, Punjab, India, with area of specialization in cryptography, position, and location computation in wireless sensor networks. He is currently working as an Associate Professor with Lovely Professional University. He has many publications in well renowned International journals and Conferences.

MRITUNJAY KUMAR RAI received the Master of Engineering degree in digital system from the Motilal Nehru National Institute of Technology, Allahabad, India, and the Ph.D. degree from the ABV Indian Institute of Information Technology and Management, Gwalior, India. He has worked as an Associate Professor with Lovely Professional University, Phagwara, India. His research interests include wireless networks, network security, and cognitive radio networks. He has published more than 50 research papers in reputed International Conferences and International Journals.

WILLIAM J. BUCHANAN is currently a Professor of cryptography. He also leads the Blockpass ID Laboratory, Edinburgh Napier University. He has authored 30 academic books and over 250 research articles. His main research interests include distributed ledger technology, identity systems, trust-based infrastructures, and cryptography. Along with this his work has supported the creation of a number of spin-out companies and international patents. He was awarded an OBE for his services to Cybersecurity, in 2017.

REJI THOMAS received the Ph.D. degree from IIT Delhi. He is currently a Professor with Lovely Professional University, Phagwara, India. His research interests include logic, memory, and energy storage devices.

MAMOUN ALAZAB (Senior Member, IEEE) received the Ph.D. degree in computer science. He is currently an Associate Professor with the College of Engineering, IT and Environment, Charles Darwin University, Australia. He is also a Cyber Security Researcher and a Practitioner with industry and academic experience. His research interests include multidisciplinary that focuses on cyber security and digital forensics of computer systems, including current and emerging issues in the cyber environment like cyber-physical systems and the Internet of Things, by taking into consideration the unique challenges present in these environments, with a focus on cybercrime detection and prevention. He has more than 100 research articles. He presented at many invited keynotes talks and panels, at conferences and venues nationally and internationally (22 events in 2018 alone). He is an Editor on multiple editorial boards, including an Associate Editor of IEEE Access and an Editor of *Security and Communication Networks* journal.