International Journal of Data Informatics and Intelligent Computing (IJDIIC)
Vol. 3, No. 2, June 2024, pp. 1~15
DOI: 10.59461/ijdiic.v3i2.104

Adoption of Blockchain Technology for Data Management of Human Resource Demands in Organizational Enterprises

Paryati[1], Prabhdeep Singh[2]
[1]University Development "Veteran" Yogyakarta, UPN "Veteran" Yogyakarta, Yogyakarta, Indonesia
[2]Department of Computer Science and Engineering, BBD University, Lucknow, Uttar Pradesh, India

Article Info

Article history:

Received February 12, 2024
Revised March 20, 2024
Accepted April 05, 2024

Keywords:

Human Resource
Organizational Enterprises
Blockchain
Smart Contracts
Proof of Work (PoW)

ABSTRACT

Human resource data accuracy has become a significant factor in assessing the effectiveness and performance of human resource management (HRM) in businesses. Numerous human resource hazards originating from asymmetric information continue to cost firms money and even put companies out of business despite the rapid progress of mobile technology and Internet technology. Blockchain is a transaction platform that makes use of the immutability qualities of immutable data records. Because of the dispersed nature of this technology, it has a broad variety of applications in numerous industries. Seeing the potential of this new technology, we picked the HRM sector since this data must be kept private and secret while still having great research value. This research presents a unique blockchain-based encryption method for establishing an HRM data method that decreases the danger of HRM data integrity. The data is authenticated using smart contracts, and data is encrypted using the proposed Improved Identity-based blowfish encryption algorithm (IIBEA) with Particle Swarm Optimization (PSO). New blocks are verified using the Proof of Work (PoW) consensus process. The suggested model's metrics are examined and compared to traditional encryption approaches. This model solves the lack of difference in the authenticity of HRM information, and it will give real and effective information to the HRM of organizational companies.

Corresponding Author: Paryati (e-mail: upnyaya@gmail.com)

1. INTRODUCTION

Enterprises are facing unprecedented pressures and problems as a result of society's fast growth and the growing trend of economic globalization. The key part of enterprise management practice is human resources, which serves as a significant carrier of information, technology, and service. HRM has a strategic value and significance for a company's future that could be substituted. Information technology's regular upgrading has become a major hidden agenda behind the fast expansion of all socioeconomic firms. Human resources are the most important manufacturing force. An organization's progress can only be hastened by retaining talent. To facilitate the accomplishment of core competitiveness in an enterprise's dynamic environment, modern HR management must merge IT with a modernized HRM notion, improve the technique, and enhance HRM effectiveness and consequences [1]. Blockchain technology has gained notoriety as the cutting-edge technology that underpins cryptocurrencies like Bitcoin and Ethereum. It's also spread, with many firms looking at its possibilities and new blockchain use cases popping up on an up-to-date basis. Its materialization has had profound effects on how data is kept and safely managed. Furthermore, almost everyone believes that blockchain will disrupt and change anything over the next few years, encompassing education, financial transactions, security, proprietary information, healthcare, and so on [2].

The fast changes in the HRM operational environment, where corporate companies collaborate with their suppliers and consumers, have highlighted the importance of interoperability of information systems. They address the challenging problem that becomes critical in frameworks such as blockchain technology, and it can snare actual data information from various parts of the human resource and managerial acquisition

process using data security and sensor-based data networks. Enterprise HRM data plays an essential role in processing and disseminating human resource data during this process. The features of distributed ledger technology are depicted in Figure 1 [3]. New technologies are having a large and rising influence on many parts of our lives, work, and enterprises. Blockchain technology is a revolutionary technology that is having a significant impact on virtually all corporate processes, including most HRM data. HR departments are now experiencing several issues as they spend a significant amount of time evaluating data security and verifying information to reduce the risk of data hacking. More technology-oriented techniques are now used to administer a company's human resource data. These Human Resource techniques are significantly more successful than traditional ways, but they can also be more costly when transactional expenses are taken into account.

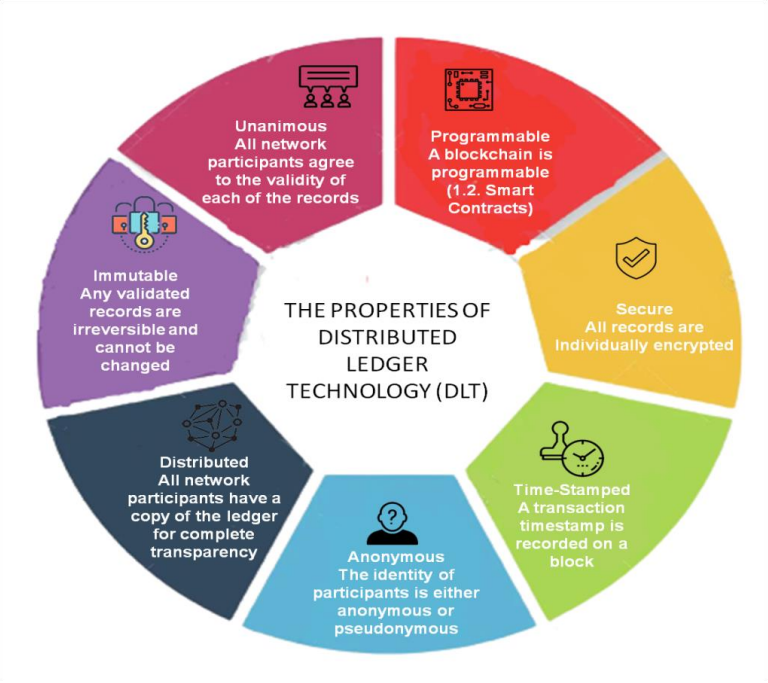

Figure 1. Properties of distributed ledger technology

There is a steady influx and outflux of new technology in the firm for traceability, which is essential due to technical improvement or system transparency. Organizations have developed new technical solutions to adapt to changes in the organizational environment to gain a competitive edge. In companies, there is an increase in the need for learning methods and good strategy programs. Blockchain technology is used to improve data security. Blockchain technology enhances the data transmission and data security of HRM data [4]. Both distribution and sharing are fundamental notions in innovation and distributed ledger technology (DLT). DLT ensures immutability, traceability, security, and transparency while improving efficiency and lowering costs for HRM. The Distributed Ledger Technology (DLT) guarantees data integrity, transparency, security, and accessibility. DLT guarantees immutability, traceability, security, and transparency. While the innovation process is about sharing skills to inform innovative effectiveness and strategies, DLT distributed data ledger that ensures integrity, track-and-trace, security, and transparency. In this post, we look at the challenges that we have when it comes to open innovation and how distributed ledgers can help us overcome them. The findings of our exploratory study suggest that DLTs can aid in the resolution of a variety of issues, including external hurdles such as contracting issues, funding issues, a lack of trust, and raw material shortages [5].

In this paper, we augment the security of the transmission process of HRM data in blockchain networks using the Improved Identity-Based Blowfish Algorithm to eliminate data security attacks.

1.1. Contribution of the study

- This study provides a novel blockchain-based encryption approach for constructing an HRM data method that reduces the risk of data integrity in HRM.
- Smart contracts are used to authenticate the data, and the suggested Improved Identity-based blowfish encryption algorithm (IIBEA) with Particle Swarm Optimization is used to encrypt it (PSO).

- The Proof of Work (PoW) consensus procedure is used to verify new blocks.
- The metrics of the proposed model are investigated and compared to standard encryption methods.
- This approach addresses the disparity in the legitimacy of HRM information, as well as providing true and useful information to corporate HRM.

The remaining sections in the paper are structured as follows. The associated literature and the problem statement are presented in Section II. The explanations of the proposed work are provided in Section III. Section IV has results and discussions. The proposed paper's conclusion is presented in section V.

2. LITERATURE REVIEW

In this section, the results of the literature review are provided, and a discussion of the data management challenges that organizational enterprises must overcome is included as well. In addition to looking at other themes, we are going to study the difficulties, peculiarities, and boundaries of the approaches. The study [6] seeks to create a human resource information management paradigm that decreases the effects of human resource information authenticity by combining classical encryption technology with Internet-dispersed technology. This method intends to address the lack of authentication of human resource information and to give genuine and efficient resolution-making information to an organization's HRM. BC's consensus process, smart contracts, accounting, and payment functionalities may all help with human resource data management.

In [7] introduced proof-of-work as an enforcement learning issue by modelling blockchain growth as a new technology, in which HRM makes the best choice possible based on the current state of the environment while a new block is added and validated. They use a deep reinforcement-learning iteration technique to create the block verification and consensus algorithm. As a result, the method makes use of the state transition determination and unpredictability of motion planning of a blowfish process, as well as the high analytical of a deep neural network, to make the blocks difficult to summate and protect the order of transmission, allowing the model to experience the many numbers of concepts across computing nodes but at the same time, it is efficient in data transmission of human resource data. According to [8], the deployment of Information Technology (IT) in the area of HRM systems is critical for any organisation to properly embrace and execute the Fourth Industrial Revolution. An algorithm for a Blockchain Recruitment Management System (BcRMS) and a Blockchain Human Resource Management System (BcHRMS) has been presented.

The researchers [9] investigated the research object, and enterprises aim to analyze and develop the HRM information system, such as the blockchain core layer and human resources information network protocol, and implement the HRM information database creation. All of the transaction records are saved, allowing people to develop in a more efficient and organized manner. The study [10] investigated how workers feel about the blockchain use of distributed ledger database technology. The data was analyzed using the log-linear analysis and fundamental frequencies. Employee perceptions of the benefits, organizational hurdles, and potential uses of blockchain in HRM were also examined in the study. The study [11] introduced the phrase co-occurrence network, which refers to a network of maps created using bibliometric data. Based on the topic clusters, four thematic clusters were formed, and two theoretical themes were produced through associations. Blockchain Framework (BSF) for Human Resources was recognized as the hidden agenda for the adoption and implementation of blockchain in the HRM domain. Later, the two theoretical themes will be supported, and the robustness of the results will be evaluated.

The study [12] objective is to use blockchain and Internet of Things (IoT) technology to monitor items from farm to fork. Consumers may obtain the data needed to make educated decisions about the human resource data and the businesses they support by building traceable and transparent data supply chains. Traceability and transparency improve customer connections, boost efficiency, and maximize data security. This firm and blockchain technology are making a case for mending and altering the world's data security system. The authors [13] proposed that the network, an algorithm-based method for selecting trustworthy resources, has been developed. Data security apps have exploded in popularity, with freshly launched services attracting tens of millions of customers. User anonymity is a characteristic that helps considerably in the development of many apps. Anonymity, on the other hand, opens the door to various misuses and abuses, such as using the network to transmit altered materials such as Trojan Horses, infections, and spam. To overcome this issue, they suggest a self-regulating system in which a robust reputation algorithm is implemented using the network. A distributed polling method is used to provide reputation sharing, which allows resource requesters to assess the credibility of a resource given by a participant before starting the download. In this way, the malicious content may spread, and it will be reduced and permanently blocked. The study [14] presented that to decrease the likelihood of malevolent activity during blockchain consensus, "Pledge," a unique Proof-of-Honesty-based consensus system. The pledge also includes transaction validation standards centred on the Internet of Things. Pledge appears to be both cost-effective and secure,

with fewer communication difficulties and transaction confirmation delays. In a variety of circumstances, data traceability with high serviceability has been frequently employed. However, throughout the data transfer process, the present traceability system frequently uses globally acknowledged cryptographic methods such as MD5 and RSA.

The authors [15] presented that Certain security flaws have been discovered in these algorithms. The SM2, SM3, and SM4 algorithms are used in the traceability system. To upgrade the HR data security representation of the transparency system of HRM based on SM2 and SM3, a certificate issue verification method must be created. At the same time, the system employs the SM4 algorithm to create a data digest-based blockchain interaction method, as well as homomorphic encryption to ensure that the data is valid. The study [16] has an objective to connect blockchain technology with HRM from the standpoint of HRM, and there have been an increasing number of studies on this topic in recent years. Blockchain technology would bring about changes in HRM, such as data security and data transmission performance evaluation; they believed that blockchain technology would bring about a more efficient social network and lower trust expenses in enterprise recruitment, and they proposed ChronoBank and CTE based on blockchain technology. Chain is a good example of a model. At all levels, the information blockchain established below is kept on the devices of nodes.

The study [17] proposed that blockchain is a revolutionary, decentralized technology that safeguards data against unwanted access. The management will be happy with the data when smart contracts are introduced. As a result, it's difficult to preserve data privacy and accountability in the system. It means that only those who have been authenticated have access to the material. The goal of this research is to reduce third-party involvement in medical health data while also increasing data security. This will increase accessibility and time efficiency throughout the process. The most important benefit is that customers will feel safer during the payment process. A smart contract was employed, as well as peer-to-peer encrypted technology. Because this document employs an immutable ledger, the hacker will be unable to obtain access to the system. They won't be able to do it.

The authors [18] proposed that typically advanced encryption algorithm (AES), international data encryption algorithm (IDEA), and data encryption standard (DES). A comparison between symmetric and asymmetric algorithms. Block Size, Protection Rate, Key Length, Rounds, and Execution Time were used to implement the algorithms. In a data set, the outcomes are more effective. "Blowfish, RSA, AES, Eclipse IDA, DSA, and other hybrid encryption schemes were introduced by the author to improve the privacy of information stored on cloud servers." They focused on giving customers the authority to choose how their data is encrypted rather than relying on third parties to do it, reducing data hacking and increasing data security. The researchers [19] investigated the fact that traditional data security sharing systems overlook the fact that numerous firms exchange human resource data transmission and data security. As a result, they devised a blockchain-based network data security sharing mechanism. The human resource data is encoded using a PCI encryption card in the hardware architecture. The CPU is utilized to access the system's external equipment, network data is stored in the DDR-SDRAM dynamic storage area, and NAND flashes static memory. The network-shared data is encrypted using the cp-abe method, and the data is shared using multi-person digital envelope technology. These two approaches aid in the development of a network data security sharing system. The system login response time, key distribution time, data encryption time, and key distribution time are all factors to consider. All areas and organizations of society have gained new development prospects and technological assistance because of the big data technology environment. HRM is increasingly significantly reliant on information technology, making information technology systems' security, reliability, and effectiveness intimately related to the safety of whole organisations and the soundness of the financial system. The intensity of data and information logic in HRM has improved immensely with the quick advancement of science and technology in various organisations, especially in the last two years, and information systems risk has surfaced as just another important sense danger in the smooth operation of HRM. The study [20] delves into the confidentiality encryption algorithm, DES encryption security algorithm, MD5 encryption protection method for financial institutions, and the privacy encryption individual's special application.

2.1. Problem Statement

The traditional HRM system has issues such as data security, human resource security, management of human resource data, staff recruitment data quality not being guaranteed, training of performance data encryption not being consistent with actual performance, all of which harm HRM and loyalty and threaten the survival and development of businesses. To accomplish the company's HRM systems, data security, data accuracy, data efficiency, and data transparency, this paper proposes an HRM mechanism based on blockchain technology and an improved identity-based blowfish algorithm(IIEBA). It has been discovered that blockchain technology and HRM systems work well together.

3. METHOD

Ensuring secured data transmission in the blockchain is very important. This paper is focused on enhancing the security of human resource data transmission in blockchain networks using the IIBEA algorithm to eliminate data hacking and prevent malicious nodes. Initially, the human resource data is preprocessed and authenticated using smart contracts. The data is encrypted before being stored in the blockchain network. The flow of our proposed work is given in Figure 2, and a detailed description is provided in this section.

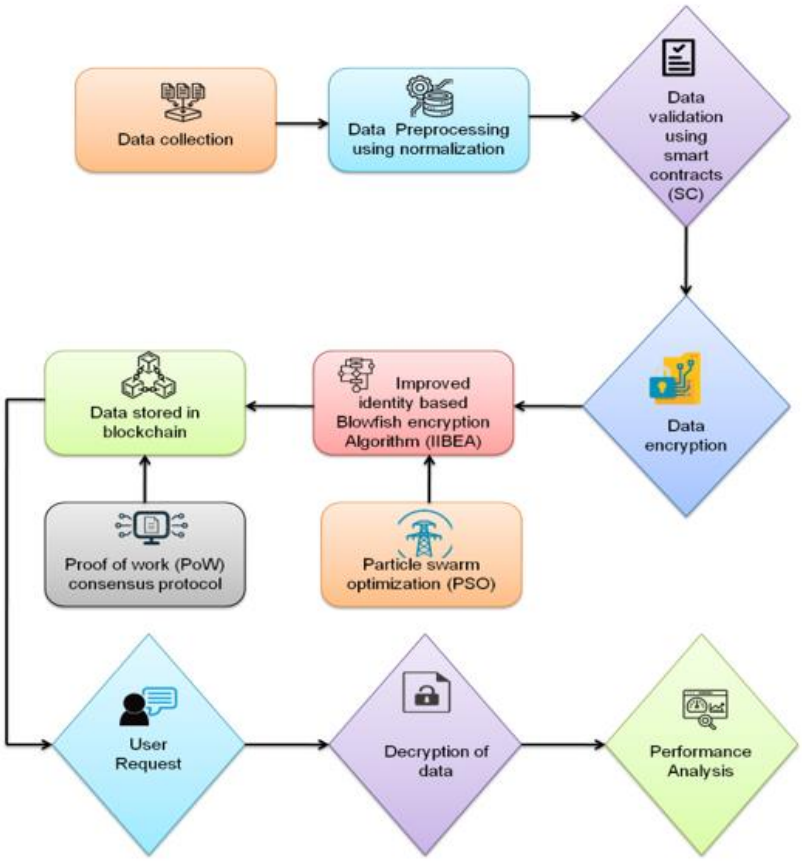

Figure 2. Proposed methodology

3.1. Dataset

HRM Organizations' data, such as client data, project data, ongoing works, etc, candidate numbers and names, as well as gender, city, work, business data, area, duration of work, and the number of hours absent, are all included in the data collection. This data set is well-organized. An online questionnaire was sent to 157 corporate social responsibility specialists to collect the information. These specialists assessed the legitimacy of 30 global corporations with over 1000 workers, as well as the execution of social responsibility activities connected to HR management. In comparison to typical businesses, these companies were picked for their considerable international presence and awareness. Because these organizations function in a variety of settings, obtaining social support is essential. Furthermore, the data set categorizes absence into 21 distinct classes or reasons for absence. Various diseases, congenital anomalies, and pregnancy are among them. The data set includes age, gender, job satisfaction, workplace environment satisfaction, educational field, job function, salary, overtime, percentage pay increase, tenure, retraining time, years in a current role, relationship status, as well as other HR data characteristics [21][22].

3.2. Preprocessing using normalization

Preprocessing transforms raw data into a format that computers can interpret and analyze as part of the data mining and data analysis process. Text, images, videos, and other real-world data are disorganized. It is typically difficult and lacks a coherent design, not to mention faults and contradictions. Normalization is a stage in the preprocessing process, a scaling method, or a mapping technique. One of the most well-known ways of standardizing data is MinMax Scaler standardization. The base guess for each component is assigned

to 0, the most extreme value to 1, and all other values to a decimal between 0 and 1. Min-Max normalization is a simple method for fitting data into a pre-defined boundary. The Min-Max normalization approach was used.

Z-score Normalization is a method that uses concepts like mean and standard deviation to obtain normalized values or ranges of data from unstructured information data. As a consequence, using the z-score variable, the data information may be normalized, as seen below:

$$v_i' = \frac{v_i - E}{\text{std}(E)} \quad (1)$$

$$\text{std}(E) = \sqrt{\frac{1}{(n-1)} \sum_{i=1}^{n} (v_i - \bar{E})^2} \quad (2)$$

$$\bar{E} = \frac{1}{n} \sum_{i=1}^{n} v_i \quad (3)$$

Therefore, the normalized values in each row above may be determined using the z score method. The standard deviation of a row is 0 if all values in that row are the same, and all of the variables in the row are set to 0. Like the normalization techniques, the z-score represents the range of values between 0 and 1. Scaling is a method that provides a range of values between -1 and 1.

3.3. Data validation using smart contracts

Smart contracts may encapsulate HRM data and legal contracts taken in management, which are then meant to represent the contractual parties' common understandings and intents in written form. Organizations' rules may be transformed into HRM programs using smart contracts. Different smart contract platforms have emerged to meet the needs of various HRM functions. Each smart contract platform has its own set of features tailored to the unique application. Ethereum, for example, is primarily designed for applications that need tokenization. Almost all platforms have the immutable program code, the decentralized ledger, and the consensus layer that make up a smart contract system. Figure 3 depicts smart contracts.

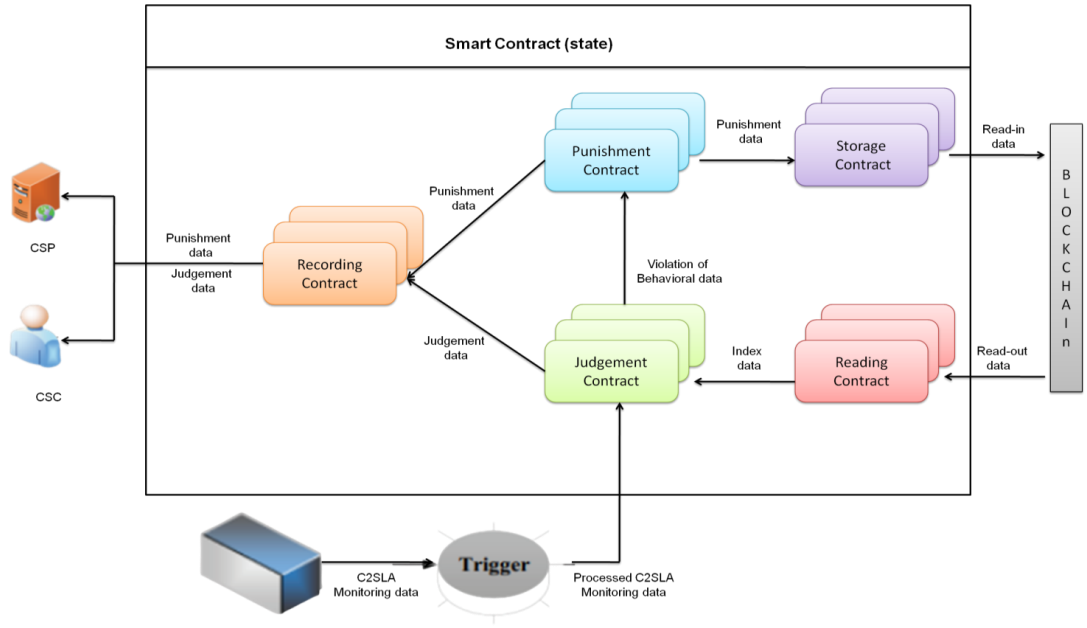

Figure 3. Smart contracts

3.4. Data encryption

The authenticated data must be encrypted to prevent it from being stolen by attackers before being stored in the blockchain. Encryption is defined as the process of changing the original data (plain text) into ciphertext (Encrypted data). In blockchain HR data or organizations' data, massive volumes of private data are handled and saved with the aid of cybersecurity, encryption guards against brute force and cyber-attacks such as malware and ransomware. Digital data transferred over the internet and through computer systems is protected by data encryption. Modern encryption methods have supplanted the old Data Encryption Standard

to safeguard data. Integrity, authentication, and non-repudiation are just a few of the security initiatives that these algorithms protect. To validate the origin of communication, the algorithms first authenticate it. They check for integrity to ensure that the contents have not been altered. Finally, the anti-non-repudiation campaign prevents senders from denying legitimate activities. Here, we apply the Improved Identity Base Blowfish Algorithm (IIBEA) to encrypt the data.

3.5. Improved Identity-Based Blowfish Encryption Algorithm (IIBEA)

We prefer to use the Improved-Identity Based Blowfish Algorithm (IIBEA) for our proposed system, which is classified as a symmetry encryption algorithm because it uses a similar hidden key to encryption and decryption messages for human resources management data. Because it uses the same key, it requires additional security against hackers and attackers. As a result, encrypt the generated key with a message digest, which is referred to as a secured hash function. Using a message digest can improve the integrity of your data. By using the message digest and preparing a long-bit encryptor, the key generated is hashed down to 160 bits. The p-box and s-box are then initialized, and the process continues until the encryptor arrives. The encryption process begins after you receive the encryptor. When encryption is achieved, a random long independent variable is generated automatically, which is unique for each ciphertext. The process of decrypting a message is the same as that of encrypting a message, but vice versa.

Blowfish is a symmetric, 64-bit block cipher with a variable length. It was created by Bruce Schnner in 1995 as a "general-purpose algorithm" to replace the ageing Data Encryption Standard (DES) encryption algorithms with a fast, free drop-in replacement. Blowfish is far quicker than DES and IDEA, plus it is unpatented and freely accessible for all purposes. However, due to its small block size, which is considered insecure, it could not completely replace DES. Its successor, Twofish, addressed the security issue with a larger block size of 128 bits. Despite this, complete Blowfish encryption has never been broken, and the method is incorporated in a wide range of cipher suites and encryption solutions. Blowfish uses a 64-bit length and a key size that ranges from 64 to 488 bits. It is made up of 16 Freistel-like iterations, all the round of which works with a 64-bit block divided into two 32-bit words. Blowfish encrypts and decrypts data using the same encryption key. Algorithm 1 shows the encryption setup using the secret key, and Algorithm 2 shows the encryption.

Algorithm 1. Setup Encryption using the secret key

1: Obtain a secret code.
2: Using Message Digests, hash the key down to 160 bits and return the byte data key.
3: Set up the p-box and s-box.
4: XOR the byte key and the p-box together.
5: Using all zero strings, encrypt the p-box and s-box.
6: Retrieve the Encryptor

Algorithm 2. Encryption

1: Create an independent value at random.
2: Allocate a byte with the amount of the original data plus an additional 8 bytes of padding.
3: Paste all bytes from the original data into a byte buffer.
4: While generating the secret key, get the encryptor created in the previous step.
5: Iterate over the buffer, increasing by 8 each time. Encrypt a 64-bit block by converting it to long, then chaining it with an independent value (IV). Return the encrypted block b. Change the independent value(IV) identical to the new block and return c. Change log to byte array and conduct the default blowfish method change and XOR procedure iv. Return the encrypted block
6: Combining byte data from the buffer
7: Convert the byte to binhex and return the binhex cipher data.

3.5.1. Particle swarm optimization

Particle swarm optimization (PSO) is a problem-solving technique that aims to improve a solution by comparing iteratively to a set of quality targets. It solves a problem by generating a group of potential answers, known as particles, and moving them around from the search space according to their position and velocity using a simple mathematical formula. The movement of a particle is governed by its local greatest position and the best-known places in the search process, which are updated as better sites are identified by other particles. As just an outcome, the swarm is predicted to move in the direction of the best options.

A swarm of possible solutions (also known as a swarm) is used in a simplified form of the PSO algorithm (called particles). A few fundamental formulas are employed to move those particles about in the

search area. The motions of the particles are determined by the finest locations in the search area, as well as the swarm's best-known location. When additional appropriate locations are discovered, they will be utilised to guide the swarm's path. The operation is repeated with the aim of achieving a satisfactory outcome, although this is not assured. Algorithm 3 depicts particle swarm optimization.

Algorithm 3. Particle swarm optimization

1. Create a uniformly distributed 'population' of agents (particles) across X.
2. Consider the goal function while evaluating the location of each particle
3. If a particle's current position is better than just its previous best position, modify it.
4. Decide which particle is the best (depending on the particle's past best positions).
5. Change the velocities of the particles.
   $V_i^{t+1} = W.V_i^t + C_1U_i^t(P_{b_1}^t - P_i^t) + C_2U_2^t(g_b^t - P_i^t)$
6. Move particles into new positions.
   $P_i^{t+1} = P_i^t + v_i^{t+1}$
7. Go to step 2 until the stopping criteria are satisfied.

3.5.2. Data storage in the blockchain

Because blockchain is decentralized, it cannot be held in a single location. As a result, it's scattered across the network on many machines and systems. The network's nodes are the systems or computers that make it up. The blockchain, which stores all of the network's transactions, is copied by each node. As a result, the blockchain system may be compared to a spreadsheet, with the data contained in each row representing the value of an address. Blockchain can be used as permissionless (e.g., Bitcoin) or permission (e.g., The Linux Foundation's Hyperledger Project). The actors in a pseudonymous or public blockchain system are unknown. Anybody can enter or leave the blockchain network at any moment, thus putting the network's security at risk. Only known and identified players expressly admitted to the blockchain network are permissioned or private blockchains. The blockchain storage structure is depicted in Figure 4. As a result, the number of harmful actors in the network is reduced. As a consequence, only authenticated and authorized actors may access the network, enhancing the system's security and meeting the needs of corporate applications.

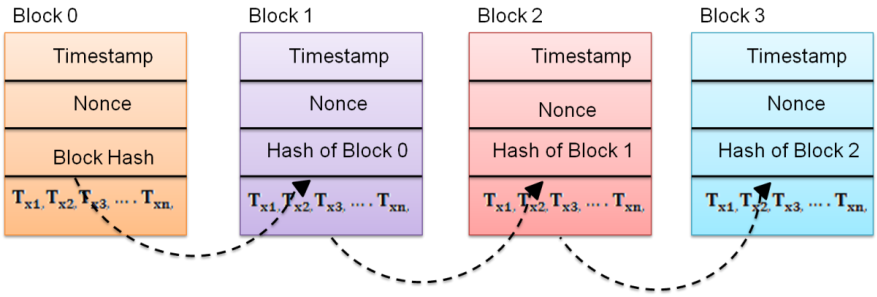

Figure 4. A blockchain structure

3.5.2.1. Proof of work (PoW) consensus protocol

Blockchain is the foundational technology underpinning numerous cryptocurrencies. The blockchain, a distributed ledger system, has gained a lot of study interest. Blockchain technology relies heavily on peer-to-peer networks and cryptography. Furthermore, consensus procedures play a crucial part in the foundations of blockchain technology. Consensus methods in blockchain systems ensure the system's security and fault tolerance. The Bitcoin white paper describing the notion of Proof of Work (PoW) was initially published by Bonneau, and Satoshi Nakamoto used it in 2008. Proof of Work is the most used cryptocurrency consensus technique. Markus Jakobsson and Ari Juels were the first to coin the term "Proof of Work." "Easy to verify but difficult to find" is the guiding philosophy here. The principle is to develop a solution that is simple to verify but difficult to locate.

Miners: Mining is the process of resolving crypto puzzles. Minor mining is the activity carried out by a node in the network. As seen in Figure 4, the new block is then uploaded to the blockchain. Here comes the proof of work as a response to a mathematical problem (crypto puzzle), which is thought to be a difficult-to-find but simple-to-verify.

Mining Pool: The mining pool is the amount of labour done by miners via a network with pooled processing power in the pooling of resources for finding new blocks. Members of the mining pool are given a "Share" amount, which is used to create a partially validated Proof of Work. As illustrated in Figure 5, the

difficulty level for miners is increased while mining in pools where it takes longer for slower miners to generate a block. Rather than discovering once every few years, it is preferable to receive incentives for each freshly produced block. This is the answer to the miners' dilemma of pooling their resources.

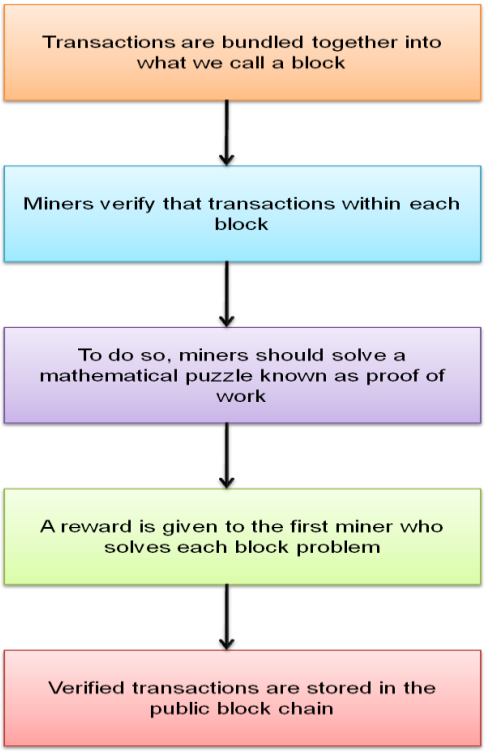

Figure 5. Flow of PoW

3.5.2.2. Decryption of data

Decryption is the method of restoring encrypted data to its original state. The encryption procedure is usually reversed in most cases. Decryption decodes the encrypted data so it can only be deciphered by an authorized user since it needs a hidden key or password. The encrypted data is divided into the relevant block lengths of the Improved Identity-Based Blowfish Encryption algorithm from top to bottom. The data may be decrypted using the equivalent encryption key if the first block is supplied to the decryption function, but the application of subkeys is reversed.

4. RESULTS AND DISCUSSION

In this paper, blockchain technology is designed using IIBEA for the storage and transmission of human resource data. This section analyzes the performance of the proposed IIBEA method in ensuring the security of data stored in the blockchain. The proposed system can give data security, data efficiency, privacy, and confidentiality security for any user's file on human resource data. The parameters are encryption time, decryption time, encryption throughput, decryption throughput, security, cost, and overall quality. The findings were compared to those obtained using existing approaches. The existing methods are "Levenberg–Marquardt and back-propagation algorithm (LMBP), Simulated Annealing Algorithm (SAA), fuzzy-human resource management-supply chain management (F-HRM-SCM), and k-means algorithm".

Calculating the amount of time needed to produce ciphertext from plaintext allows one to arrive at the time required for encryption. It can be shown in Figure 6 that the amount of encryption time needed for the suggested model to process each file is the smallest possible amount.

The amount of time needed to transform ciphertext into plain text is included into the calculation of the decryption time Figure 7. In the course of the investigation, it was discovered that the suggested model hybrid encryption algorithm for large data security has a decryption time that is noticeably shorter in comparison to the times required by other encryption algorithms.

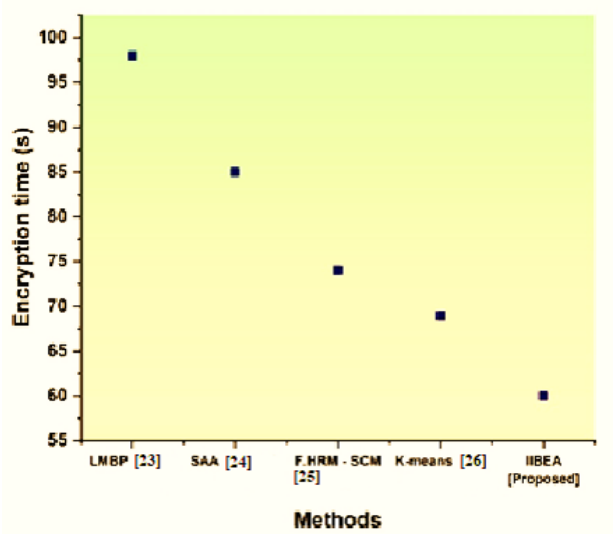

Figure 6. Encryption time

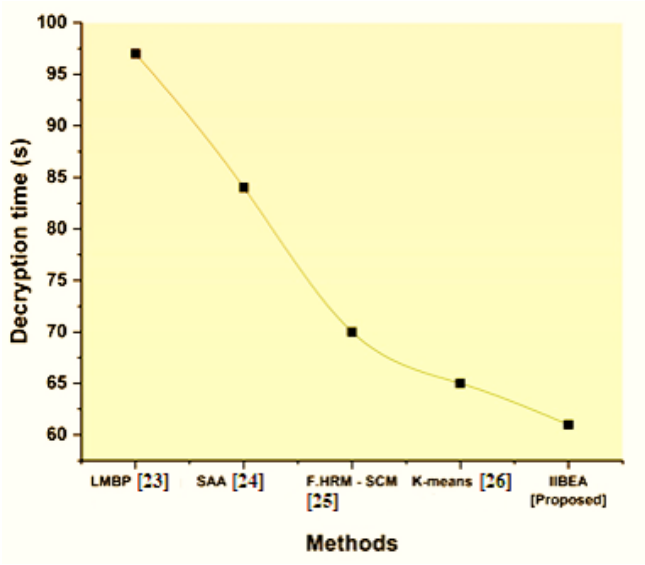

Figure 7. Decryption time

Calculations are done to determine the throughput for both the encryption and decryption procedures in Figures 8 and 9. When encrypting data, the throughput may be determined by calculating the ratio of the amount of time it takes to finish the procedure to the total size of the text being encrypted. The ratio of the entire amount of ciphertext to the amount of time required for the decryption process is used to calculate the throughput for decryption. The research reveals that the suggested encryption technique had the highest throughput when compared to other algorithms because it required the smallest amount of text and the least amount of processing time.

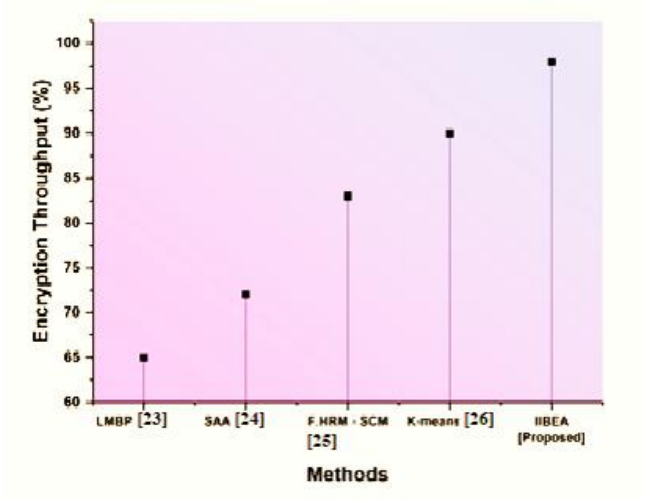

Figure 8. Encryption throughput

Whereas, while using traditional encryption techniques, the amount of text being encrypted grew, and both the encryption and decryption processes took longer. Because of this, the throughput of traditional encryption techniques was lowered, and their performance suffered when compared to that of the suggested encryption algorithm.

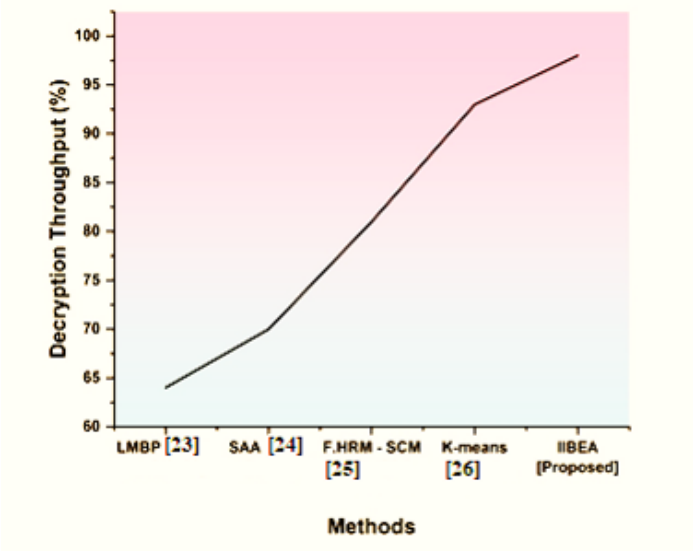

Figure 9. Decryption throughput

Hacking or system management may easily compromise the present system's security. Information leaks and data manipulation are exceedingly uncommon since Blockchain systems are safeguarded by a double-layered key and hashed encryption. Due to the distributed structure of the system, information changes can be readily traced, and original data may be recovered without causing significant loss. As previously said, blockchain adds an added degree of security. Figure 10 shows the comparison of security for existing and proposed work.

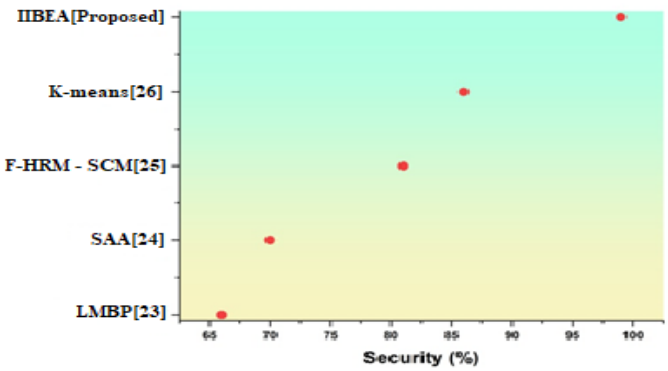

Figure 10. Comparison of Security for existing and proposed work

In comparison to previous systems, our system requires a significant quantity of storage, has a higher power consumption rate, and requires more investment during the initial setup phase. However, the return on investment should be significantly larger in the long run. As a result, our systems will save money over time. It will also avoid any extra costs incurred as a result of incorrect hiring utilizing current methods. The cost of existing and proposed work is compared in Figure 11.

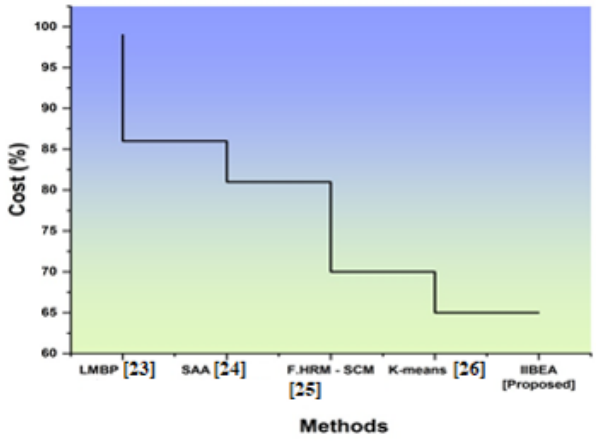

Figure 11. Comparison of cost for existing and proposed work

Machines ensure the quality of recruiting and HRM operations in our suggested system. With total transparency and security, our system can handle, store, verify, and rank information. There is no risk of quality deterioration since our suggested system makes no fictitious or biased conclusions. Figure 12 compares the overall quality of existing and proposed work.

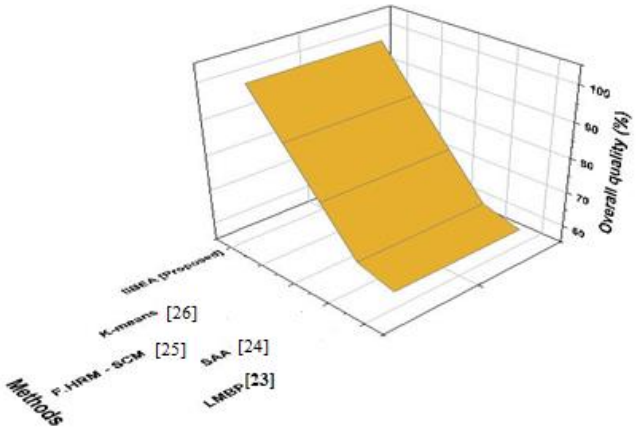

Figure 12. Comparison of overall quality for existing and proposed work

4.1. Discussion

In LMBP [23], to improve the external validity of the study findings, a sample selection procedure was used, and the number of samples was increased. - The method of influencing enterprise performance is reduced to some degree by using the effectiveness variable as an intermediate variable, and the effect of regulatory variables is completely addressed in this process. Conduct an extensive empirical study on a certain industry. These are some limitations of the LMBP algorithm. Simulated annealing (SA) [24], F-HRM-SCM [25] is a probabilistic approach for determining the optimum solution of a stored algorithm. It is a metaheuristic that approximates global optimization in a large search space for an optimization problem. It takes a long time to anneal repeatedly with a schedule, especially if the cost function is difficult to compute. The classic k-means algorithm [26] has many drawbacks when it comes to the processing of vast amounts of data, including poor computational efficiency and high temporal complexity. Consequently, we employ smart contracts that have been validated, and the data is encrypted using a new technique called the Improved Identity-based blowfish encryption algorithm (IIBEA) with Particle Swarm Optimization (PSO).

5. CONCLUSION

The most difficult challenges are user authentication and data security. As a result, this research proposes an important and scalable access control mechanism. Moreover, this method utilizes an Improved Identity-Based Blowfish Encryption Algorithm encryption mechanism to provide data security for consumers and the central authority, not only to provide data security against a cloud service provider but also to provide data security against a semi-trusted cloud service provider. Furthermore, the partial signing architecture used in this technique can lower the user's computation cost on the cloud server, making it more efficient and acceptable for devices with limited resources.

Improved Identity-Based Blowfish Encryption Algorithm (IIBEA) is used to transport data securely. When an authorized user submits a request to the cloud, the files attached to it are encrypted and sent to the consumer based on their size. The data user can then decode the data using the IIBEA approach's key. The findings reveal that the suggested IIBEA approach is successful in terms of the authenticity of data, encryption time, decryption time, encryption throughput, decryption throughput, security, cost, and overall quality and that it beats the classic LMBP, SAA, F-HRM-SCM, and k-means algorithm method. The recommended study's future scope might include information sharing with re-encryption and transparency, performance encryption, and safeguards property-based encryption. In the future, we may investigate utilizing several techniques to exchange information in these areas and introduce optimization techniques to improve other performance metrics.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest in this work.

REFERENCES

[1] X. Wang, L. Feng, H. Zhang, C. Lyu, L. Wang, and Y. You, “Human Resource Information Management Model based on Blockchain Technology,” in *2017 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, IEEE, Apr. 2017, pp. 168–173. doi: 10.1109/SOSE.2017.34.

[2] P. T. Duy, D. T. T. Hien, D. H. Hien, and V.-H. Pham, “A survey on opportunities and challenges of Blockchain technology adoption for revolutionary innovation,” in *Proceedings of the Ninth International Symposium on Information and Communication Technology - SoICT 2018*, New York, New York, USA: ACM Press, 2018, pp. 200–207. doi: 10.1145/3287921.3287978.

[3] K. Pal and A.-U.-H. Yasar, “Internet of Things and Blockchain Technology in Apparel Manufacturing Supply Chain Data Management,” *Procedia Comput. Sci.*, vol. 170, pp. 450–457, 2020, doi: 10.1016/j.procs.2020.03.088.

[4] O. Fachrunnisa and F. K. Hussain, “Blockchain-based human resource management practices for mitigating skills and competencies gap in workforce,” *Int. J. Eng. Bus. Manag.*, vol. 12, p. 184797902096640, Jan. 2020, doi: 10.1177/1847979020966400.

[5] G. Jain, N. Sharma, and A. Shrivastava, “Enhancing training effectiveness for organizations through blockchain-enabled training effectiveness measurement (BETEM),” *J. Organ. Chang. Manag.*, vol. 34, no. 2, pp. 439–461, Mar. 2021, doi: 10.1108/JOCM-10-2020-0303.

[6] R. R. Chandan, A. Balobaid, N. L. S. Cherukupalli, G. H L, F. Flammini, and R. Natarajan, “Secure Modern Wireless Communication Network Based on Blockchain Technology,” *Electronics*, vol. 12, no. 5, p. 1095, Feb. 2023, doi: 10.3390/electronics12051095.

[7] J. You, “Curvetime: A blockchain framework for Artificial Intelligence computation,” *Softw. Impacts*, vol. 13, p.

100314, Aug. 2022, doi: 10.1016/j.simpa.2022.100314.
[8] M. H. Onik, M. H. Miraz, and Chul-Soo Kim, "A Recruitment and Human Resource Management Technique Using Blockchain Technology for Industry 4.0," in *Smart Cities Symposium 2018*, Institution of Engineering and Technology, 2018, pp. 3 (6 pp.)-3 (6 pp.). doi: 10.1049/cp.2018.1371.
[9] M. Kun, Z. Zhibo, L. Tao, Q. Shilin, and H. Mingxia, "Research and Application in Human Resources Information System of Electric Power Enterprises Based on Blockchain Integration," in *2021 3rd Asia Energy and Electrical Engineering Symposium (AEEES)*, IEEE, Mar. 2021, pp. 984–987. doi: 10.1109/AEEES51875.2021.9403112.
[10] H. Mishra and M. Venkatesan, "Blockchain in human resource management of organizations: an empirical assessment to gauge HR and non-HR perspective," *J. Organ. Chang. Manag.*, vol. 34, no. 2, pp. 525–542, Mar. 2021, doi: 10.1108/JOCM-08-2020-0261.
[11] A. N. Mohammad Saif and M. A. Islam, "Blockchain in human resource management: a systematic review and bibliometric analysis," *Technol. Anal. Strateg. Manag.*, vol. 36, no. 4, pp. 635–650, Apr. 2024, doi: 10.1080/09537325.2022.2049226.
[12] D. Bumblauskas, A. Mann, B. Dugan, and J. Rittmer, "A blockchain use case in food distribution: Do you know where your food has been?," *Int. J. Inf. Manage.*, vol. 52, p. 102008, Jun. 2020, doi: 10.1016/j.ijinfomgt.2019.09.004.
[13] E. Damiani, D. C. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante, "A reputation-based approach for choosing reliable resources in peer-to-peer networks," in *Proceedings of the 9th ACM conference on Computer and communications security*, New York, NY, USA: ACM, Nov. 2002, pp. 207–216. doi: 10.1145/586110.586138.
[14] I. Makhdoom, F. Tofigh, I. Zhou, M. Abolhasan, and J. Lipman, "PLEDGE: An IoT-oriented Proof-of-Honesty based Blockchain Consensus Protocol," in *2020 IEEE 45th Conference on Local Computer Networks (LCN)*, IEEE, Nov. 2020, pp. 54–64. doi: 10.1109/LCN48667.2020.9314794.
[15] S. Zhang, H. Meng, X. Li, W. Liu, and B. Liu, "Hunion Traceability: A New Type of Blockchain Traceability System Based on SM2, SM3 and SM4," in *2021 4th International Conference on Blockchain Technology and Applications*, New York, NY, USA: ACM, Dec. 2021, pp. 107–115. doi: 10.1145/3510487.3510503.
[16] A. Pal, C. K. Tiwari, and N. Haldar, "Blockchain for business management: Applications, challenges and potentials," *J. High Technol. Manag. Res.*, vol. 32, no. 2, p. 100414, Nov. 2021, doi: 10.1016/j.hitech.2021.100414.
[17] L. Li, H. Zhang, and Y. Dong, "Mechanism Construction of Human Resource Management based on Blockchain Technology," *J. Syst. Sci. Inf.*, vol. 9, no. 3, pp. 310–320, Jul. 2021, doi: 10.21078/JSSI-2021-310-11.
[18] K. T. Akhter Md Hasib *et al.*, "Electronic Health Record Monitoring System and Data Security Using Blockchain Technology," *Secur. Commun. Networks*, vol. 2022, pp. 1–15, Feb. 2022, doi: 10.1155/2022/2366632.
[19] F. Thabit, A. P. S. Alhomdy, A. H. A. Al-Ahdal, and P. D. S. Jagtap, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," *Glob. Transitions Proc.*, vol. 2, no. 1, pp. 91–99, Jun. 2021, doi: 10.1016/j.gltp.2021.01.013.
[20] X. Lu, P. Liu, Y. Ke, and H. Zhang, "Network data security sharing system based on blockchain," *Multimed. Tools Appl.*, vol. 80, no. 21–23, pp. 31887–31906, Sep. 2021, doi: 10.1007/s11042-021-11183-6.
[21] A. K. M. B. Haque, B. Bhushan, and G. Dhiman, "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends," *Expert Syst.*, vol. 39, no. 5, Jun. 2022, doi: 10.1111/exsy.12753.
[22] C. del-Castillo-Feito, A. Blanco-González, and F. Hernández-Perlines, "The impacts of socially responsible human resources management on organizational legitimacy," *Technol. Forecast. Soc. Change*, vol. 174, p. 121274, Jan. 2022, doi: 10.1016/j.techfore.2021.121274.
[23] L. Qiang and Z. Zhongwei, "Relationship Model between Human Resource Management Activities and Performance Based on LMBP Algorithm," *Secur. Commun. Networks*, vol. 2022, pp. 1–11, Jan. 2022, doi: 10.1155/2022/1125084.
[24] M. Xu and C. Li, "Data Mining Method of Enterprise Human Resource Management Based on Simulated Annealing Algorithm," *Secur. Commun. Networks*, vol. 2021, pp. 1–9, Oct. 2021, doi: 10.1155/2021/6342970.
[25] M. T. Alshurideh *et al.*, "RETRACTED ARTICLE: Fuzzy assisted human resource management for supply chain management issues," *Ann. Oper. Res.*, vol. 326, no. S1, pp. 137–138, Jul. 2023, doi: 10.1007/s10479-021-04472-8.
[26] Q. Sun, T. Wu, and J. Hua, "Design of Distributed Human Resource Management System of Spark Framework Based on Fuzzy Clustering," *J. Sensors*, vol. 2022, pp. 1–9, Mar. 2022, doi: 10.1155/2022/4827021.

BIOGRAPHIES OF AUTHORS

Paryati is a Lecturer and Assistant Professor at the National Development University "Veteran" Yogyakarta, Indonesia. She has completed a bachelor's degree in Informatics Management and Computer Engineering Study Program. She completed her master's in computer science at Gajah Mada University as the fastest-graduating student and cum laude. She is currently completing her doctoral preparation. She has been a certified Microsoft Innovative educator trainer since 2011. Her research interests are genetic algorithms, artificial intelligence, expert systems, data mining, machine learning, deep learning systems, fuzzy logic, data analysis and smart city information

systems. She has published 97 papers at international and national conferences as well as in the indexed journals Scopus, Springer, IEEE, IGI Global, Taylor & Francis, and others. She has 4 book chapters at Taylor & Francis, 3 books at Betham publisher, 7 books at LAMBERT publisher. She is a peer reviewer in various international journals. She is a member of technical functional bodies in APTIKOM, HMI, IASR and others. She has published 13 COPYRIGHT Books and 4 PATENTS. She is a reviewer for the journals ABAARJ, AJASR, AJCR, AJOMCOR, AJPAM, AJPAS, ARJOM, CJAST, GPH, IJB, JAMCS, MULTIDICIPLINARY, JPRI. She has been a speaker for 5 webinars, 5 international conferences, 5 international workshops, and soft skills workshops at home and abroad. She has received various research and community service grants at national and international levels. She can be contacted at email: upnyaya@gmail.com.

Prabhdeep Singh received a B.Tech (Computer Science and Engineering) from Saroj Institute of Technology and Management, Lucknow, affiliated with U.P.T.U., U.P., India, M. Tech. (Computer Science) and Pursuing Ph.D. (Computer Science and Engineering) from Amity School of Engineering and Technology Lucknow, Amity University Uttar Pradesh, India. His research interests include cloud computing, data security, machine learning, data mining and warehousing, scheduling and optimization. He has published a number of research papers in journals of national and international reputation. He can be contacted at email: prabhdeepcs@gmail.com