AI and ML-Based Secure Employee Data Management with Blockchain: Applications of Distributed MPC and Sparse Matrix Algorithms in HRM

Rajani Priya Nippatla,
Kellton Technologies Inc, Texas, USA
rnippatla@gmail.com

Harleen KAUR
Full Professor, Fr Research Fellow United Nations (Tokyo), TWAS Visiting Professor,Fellow(IETE)
harleenjamiahamdard@gmail.com

ABSTRACT

Background Information: In the contemporary digital era, the secure administration of employee data has become essential. Conventional HR systems are vulnerable to cyber assaults, requiring strong, decentralised alternatives. Emerging technologies such as AI, ML, Blockchain, Distributed MPC, and Sparse Matrix algorithms offer secure, efficient, and scalable solutions for the management of sensitive HR data, while maintaining privacy and compliance.

Objectives: The main purpose is to create a framework utilising AI and ML, incorporating Blockchain, Distributed MPC, and Sparse Matrix algorithms, to ensure the security of employee data management. The technology augments decision-making, safeguards data privacy, guarantees regulatory compliance, and boosts operational efficiency in HR procedures.

Methods: The suggested system utilises artificial intelligence and machine learning for data analysis, blockchain for safe and immutable storage, distributed multi-party computation for private calculations, and sparse matrix algorithms for optimising extensive datasets. These technologies converge to establish a secure, decentralised, and scalable human resources data management system.

Results: The technology strengthens security, guarantees GDPR compliance, improves data retrieval, and streamlines HR operations. It offers predictive insights and markedly diminishes the danger of data breaches while facilitating effective data processing.

Conclusion: The suggested system effectively secures employee data management through the integration of AI, ML, Blockchain, Distributed MPC, and Sparse Matrix algorithms. This method improves decision-making and data security, offering a scalable and safe solution for contemporary HR departments, particularly in a digital environment.

Keywords: Artificial Intelligence, Machine Learning, Blockchain Technology, Distributed Multi-Party Computation, Sparse Matrices, Human Resource Management, Security, Data Governance, General Data Protection Regulation, Privacy.

1. INTRODUCTION

In the rapidly expanding digital landscape, the management of employee data has become essential for enterprises worldwide. Human Resource Management (HRM) departments manage significant quantities of sensitive data, including personal information, employment records, performance measures, and payroll data. As corporations digitize documents, the efficient security and management of this sensitive data is a considerable problem. Conventional solutions frequently fall short in guaranteeing data security, privacy, and integrity because of the escalating complexity of cyber threats. This is where nascent technologies such as Artificial Intelligence (AI), Machine Learning (ML), and Blockchain are relevant. These technologies have the capacity to revolutionize HRM by delivering sophisticated solutions for secure employee data management. The integration of AI and ML algorithms with Blockchain technology promotes data management security and transparency while facilitating decentralized data control, hence removing dependence on a singular central authority.

In this context, Distributed Multi-Party Computation (MPC) and Sparse Matrix Algorithms have become pivotal in transforming safe employee data management. By utilizing these technologies, HRM systems may guarantee data confidentiality, enhance processing efficiency, and provide predictive insights for improved management of workforce-related operations. This introduction seeks to explore the importance of AI, ML, Blockchain, and related algorithms, such as Distributed MPC and Sparse Matrix algorithms, in establishing a secure, efficient, and transparent system for employee data management in Human Resource Management. Employee data includes personal identification numbers, financial information, and health records. The secrecy of this data is crucial for adherence to privacy regulations and preserving employee trust. Conventional systems, typically reliant on centralized data storage, are susceptible to security threats including hacking, data leaks, and unauthorized access.

As organizations increasingly digital, HR departments want technologies that rapidly store and handle data while simultaneously providing rigorous security measures. Furthermore, the growing dependence on remote work and cloud-based solutions has heightened the necessity for sophisticated cybersecurity protocols in human resource management. The integration of AI and ML with Blockchain technology provides a robust solution to this issue by establishing decentralized systems that encrypt data, distribute it across numerous nodes, and validate it through consensus procedures. This guarantees data integrity and reduces the likelihood of unauthorized manipulation or disclosure. AI and ML enhance predictive security models that identify anomalies and possible threats in real time, so averting security breaches before they transpire. Artificial Intelligence and Machine Learning have demonstrated their transformational capabilities across multiple industries, including Human Resource Management. In the domain of personnel data management, these technologies facilitate automated data processing, predictive analytics, and informed decision-making. AI-driven algorithms can automate tedious HR functions such as resume sorting, performance data analysis, and offering training programs according to an employee's prior experiences and learning trajectory. Conversely, Machine Learning can forecast staff attrition, evaluate job happiness, and identify potential compliance concerns based on past data trends.

In the context of employee data management, AI and ML can alleviate the administrative workload on HR teams while facilitating more precise, prompt, and data-informed decision-making. These solutions enhance security by continuously monitoring data access patterns, identifying potential breaches, and responding in real-time to mitigate threats. Blockchain technology, because to its decentralized characteristics, provides substantial benefits for the secure handling of employee data. Blockchain guarantees the immutability and transparency of recorded data by distributing it across numerous nodes in a network and employing cryptographic hashing. This trait is especially advantageous for HR departments managing very sensitive data. In the realm of Human Resource Management, Blockchain can facilitate safe identity verification, guaranteeing that only authorized personnel access critical information. It facilitates immutable records of employment history, credentials, and certificates, which can be validated independently of intermediaries. Moreover, smart contracts—self-executing agreements with conditions encoded directly—can facilitate payroll management, benefits distribution, and employment contracts, automating these functions while guaranteeing transparency and security.

Distributed Multi-Party Computation (MPC) is a cryptographic method enabling several participants to collaboratively compute a function based on their inputs while maintaining the confidentiality of those inputs. MPC facilitates HR departments in collaborating and sharing sensitive employee data, such as wage information and performance metrics, while safeguarding the underlying data from unwanted access. By decentralizing the computational process, MPC mitigates the risk of data exposure, safeguarding sensitive employee information while facilitating collaborative decision-making. This is particularly crucial in multinational firms where HR departments in several areas must exchange data while safeguarding its integrity and privacy.

Sparse Matrix Algorithms are mathematical methods employed to effectively handle extensive datasets characterized by a substantial quantity of zero values or extraneous information. In Human Resource Management, employee data might be extensive; nevertheless, a significant portion of this information is frequently not pertinent. Sparse Matrix Algorithms enhance the efficiency of data storage and processing, minimizing computational overhead and augmenting system performance. When combined with AI and ML models, Sparse Matrix Algorithms enable HR departments to evaluate extensive datasets more effectively, facilitating the extraction of significant insights without the encumbrance of extraneous information. This is especially beneficial in domains like employee performance assessment, where extensive historical data must be analyzed to discern trends and generate precise forecasts.

The key objectives are:

- The application of AI and ML in Human Resource Management improves decision-making, predictive analytics, and security. These tools automate data processing and deliver real-time insights, enhancing HR operations.
- Blockchain for Security: Blockchain provides decentralized, immutable data storage, guaranteeing the security and transparency of employee records, payroll, and identity verification.

- Distributed MPC: This method facilitates the sharing of sensitive data for collaborative computations while safeguarding the underlying information, hence maintaining privacy in cooperative HR activities.
- Sparse Matrix Algorithms enhance the efficiency and scalability of HR data analysis by optimizing the processing of extensive, intricate datasets.
- The aim of incorporating AI, ML, Blockchain, MPC, and Sparse Matrix Algorithms in HRM is to establish a secure, efficient, and transparent framework for managing employee data, enhancing decision-making, and protecting sensitive information.

Kim et al. (2020) emphasise the scarcity of research about blockchain applications in human resource management and the inadequate performance evaluation of current systems. They propose a privacy-preserving distributed ledger framework to manage global human resource records and overcome these inadequacies. Utilising blockchain, the framework guarantees secure, decentralised storage and management of personnel records, safeguarding privacy while ensuring transparency and responsibility. This method facilitates global, cross-border data sharing while preserving data integrity. The proposed blockchain approach tackles the issues of scalability and anonymity, providing a strong alternative to conventional HR administration solutions.

Fachrunnisa and Hussain (2020) highlight the restricted implementation of blockchain technology in human resources operations and underscore the necessity for cohesive solutions to rectify inefficiencies in HR processes. They propose a blockchain-based architecture for human resource management designed to address the skills and competencies gap in the workforce. This system utilises blockchain's transparency and security to optimise recruitment, personnel evaluation, and skill monitoring, guaranteeing that competencies are precisely documented and verifiable. Integrating blockchain into HR procedures boosts staff development, mitigates skill mismatches, and promotes effective personnel management, hence contributing to long-term organisational progress.

2. LITERATURE SURVEY

In a period characterized by demand uncertainty and intricate markets, firms endeavor to integrate and optimize comprehensive supply chain activities. **Elbegzaya (2020)** asserts that AI and machine learning are progressively employed in demand planning and forecasting, with accuracy rates of up to 85%. Nonetheless, its utilization in other domains of supply chain management (SCM), including MRP, MPS, and predictive maintenance, is still restricted. This research examines AI's capacity to improve decision-making in supply chain management by tackling intricate relationships and facilitating real-time problem-solving. This document evaluates current AI applications, supply chain management models, and data prerequisites, while examining future opportunities for AI to revolutionize conventional supply chain management techniques.

Mazilescu and Micu (2019) assert that Intelligent Automation (InA) is the further advancement beyond Robotic Process Automation (RPA) in optimizing enterprise-level business operations. InA amalgamates diverse technologies such as artificial intelligence, cloud computing, and Big Data, facilitating real-time decision-making and enhancing process efficiency. The document highlights the role of Cognitive Technologies (CTs) and digital

workers in automating manual jobs and facilitating seamless interactions between individuals and information systems. By utilizing these technologies through collaborative development, firms can attain a harmonious integration of human and machine, thereby substantially enhancing the value added to business processes.

Chowdhury (2021) characterizes auditing as a systematic and impartial evaluation of facts pertaining to economic activities to verify conformity with set criteria, thereafter conveying the findings to pertinent stakeholders. Auditors deliver expert assessments derived from their impartial evaluation of financial accounts and management claims. Expert systems (ESs), which integrate specialized expertise to identify prospective problems, are progressively utilized to improve audit quality. In Bangladesh, numerous organizations depend on bespoke software for transaction documentation, inventory oversight, and financial reporting, with service providers customizing these systems to fulfill particular client requirements, hence enhancing the audit process through automation and precision.

Ghosh et al. (2021) underscore the increasing impetus on industrial enterprises to innovate through the utilization of the Industrial Internet of Things (IIoT) and nascent digital technologies. Corporate digital entrepreneurship is recognized as a crucial difference in a competitive and disruptive environment. Nevertheless, industrial managers sometimes lack a precise framework for fostering product and process innovation. This study presents a conceptual framework for corporate digital entrepreneurship, emphasizing three essential components: business model transformation, operational model transformation, and culture transformation. The authors examine practical implications and the influence of digital technologies on promoting creativity within businesses through three case studies.

Persis et al. (2021) examine the influence of Circular Economy (CE), Internet of Things (IoT), and Ethical Business Practices (EBP) (CE-IoTEBP) within the volatile, unpredictable, complex, and ambiguous (VUCA) environment, specifically targeting the food processing sector. The research found 79 parameters affecting CE-IoTEBP acceptance, which were then reduced to 39 through Ant Colony Optimization (ACO) for enhanced decision-making efficacy. Fuzzy Artificial Neural Networks (FANN) categorized these parameters according to their levels of influence, resulting in a conclusive assessment of the intention to implement CE-IoTEBP. A deployment model was created to assist organizations in enhancing low-performing variables, serving as a reference for both academia and industry.

Butcher et al. (2021) investigate the development of Artificial Intelligence capabilities in sub-Saharan Africa (SSA), concentrating on three principal stakeholders: Higher Education and Training Institutions, Governments, and the wider AI community. The research, backed by the AI4D Africa initiative, encompasses a thorough literature assessment and insights derived from a UNESCO report. The study underscores the significance of stakeholder engagement in cultivating a dynamic AI ecosystem, highlighting the necessity of capacity building in essential domains to propel national advancement. The results emphasize the necessity for collaborative initiatives to cultivate AI knowledge and infrastructure throughout the area, thereby preparing SSA for future progress in AI research.

Gao et al. (2021) introduce BSSPD, a blockchain-based security sharing framework for personal data, which incorporates blockchain technology, ciphertext-policy attribute-based

encryption (CP-ABE), and the InterPlanetary File System (IPFS). In this decentralised, user-focused framework, data proprietors encrypt and store information on IPFS, utilising blockchain to disseminate access keys according to defined policies. Only authorised individuals who satisfy the access criteria are permitted to download and decode the data. The framework facilitates precise access control and permits revocation at the attribute level. Ciphertext keyword search is employed for data retrieval to augment privacy. The simulation on the EOS blockchain illustrated the scheme's viability and operational efficiency.

Pinna et al. (2020) offer a Blockchain-Oriented Software system for the management of the construction workforce, emphasising worker safety and sustainable human resource practices. The solution employs Blockchain technology to provide data integrity, transparency, and immutable time stamps for documented activities. It executes smart contracts, automates adherence to legal obligations, and streamlines job posting and application procedures. The design adheres to the Blockchain-Oriented Software Engineering (BOSE) methodology and the Agile Blockchain-Centered Development (ABCDE) framework. The system, implemented on Ethereum via the ERC721 standard, is assessed for sustainability and juxtaposed with centralised solutions, emphasising its benefits in transparency, cost-effectiveness, and user interface efficacy.

Sifah et al. (2020) introduce BEMPAS, a decentralised system for evaluating employee performance that employs blockchain technology for Smart City governance. BEMPAS utilises blockchain technology to enhance tamper-resistance, accountability, transparency, and security, hence addressing trust issues in centralised systems. The system incorporates a triadic model—ID-Chain, Behaviour Chain, and Credit Chain—into a cohesive blockchain for monitoring employee performance. An automated game-based evaluation method is utilised for objective decision-making. The system's Proof of Concept (PoC), constructed on Hyperledger Fabric, illustrates its capacity to improve trust, privacy, and accountability, offering a transparent and secure alternative for evaluating government worker performance in Smart City contexts.

Truong et al. (2019) offer a blockchain-based platform for the management of personal data in compliance with GDPR, tackling the issue of confirming continuous adherence to GDPR by service providers. The platform utilises blockchain and smart contracts to offer decentralised solutions for service providers and data owners, guaranteeing data provenance, transparency, and secure processing. Data proprietors govern consent for data utilisation, with all actions permanently recorded on a distributed ledger. Service providers that adhere to regulations receive endorsement from the blockchain, with infractions readily identifiable. The platform, implemented on Hyperledger Fabric, illustrates feasibility and effectiveness in achieving GDPR compliance and secure handling of personal data.

Ganesan (2020) study focusses on employing machine learning methodologies in artificial intelligence to enhance fraud detection in IoT-based financial transactions. The expansion of IoT in financial services has increased the demand for sophisticated fraud detection. Ganesan illustrates the efficacy of techniques like as neural networks and decision trees in detecting transactional irregularities. The paper presents scalable fraud detection systems that respond to evolving risks through the analysis of real-time IoT data. This work emphasises adaptive

continuous learning models that address emerging fraudulent behaviours, offering a comprehensive framework to safeguard financial transactions in IoT environments and mitigate fraud risks in these intricate systems.

The study conducted by **Gudivaka (2021)** investigates the incorporation of AI and big data to improve music education via data-driven instructional tools. To meet the demand for customised music education, Gudivaka employs AI algorithms to examine extensive information concerning student learning behaviours, performance indicators, and practice routines. This analysis enables AI technologies to provide customised feedback and enhancement suggestions, hence boosting teaching and learning experiences. The study emphasises the significance of big data in discerning learning trends beyond conventional approaches, facilitating curriculum enhancement. Gudivaka's work integrates AI with big data to provide a framework for accessible and effective AI-assisted music teaching.

Ayyadurai (2021) study investigates the function of big data analytics in overseeing supply chain dynamics in e-commerce, particularly addressing challenges associated with manufacturer invasion and channel conflict. Ayyadurai examines how data analytics technologies might enhance the precision of demand forecasts and provide improved information exchange between producers and retailers, thereby mitigating potential conflicts in supply chain operations. The research emphasises the influence of demand-information sharing on supply chain transparency and efficiency, along with its function in equilibrating power dynamics between manufacturers and retailers. Ayyadurai illustrates through case studies and data analysis how big data may foster mutually beneficial outcomes in e-commerce supply chains, ensuring that manufacturers refrain from intruding on retail channels while enhancing inventory management and demand response. This study offers a framework for e-commerce platforms to utilise big data in tackling conventional supply chain issues and enhancing collaboration among supply chain participants.

Basani (2021) investigated the function of artificial intelligence (AI) in improving cybersecurity and cyber defence. The research underscores AI's capacity to adapt, learn, and anticipate threats, rendering it an effective instrument for protecting infrastructure and digital assets. AI substantially enhances cybersecurity operations through the automation of risk detection, response, and mitigation. The study examines the progression of AI in cybersecurity, assesses essential AI tools and platforms, and analyses the benefits and obstacles of incorporating AI into current systems. This study highlights AI's capacity to enhance overall cyber resilience.

Alagarsundaram (2021) proposed a blockchain-based data sharing strategy that integrates RFID technology to improve big data medical research and assure secure exchange of physiological signal data. The model utilises RFID for real-time data acquisition and blockchain for decentralised, secure communication, overcoming the shortcomings of conventional centralised systems regarding data integrity, security, and patient confidentiality. Furthermore, fog computing facilitates scalability and robustness through the management of substantial data volumes. The study underscores the model's capacity to enhance the efficiency and reliability of data sharing, advantageous for both patients and medical research.

Sareddy (2021) examined the utilisation of sophisticated quantitative models, such as Markov Analysis, linear functions, and logarithms, to tackle intricate challenges in Human Resource Management (HRM). The research emphasises its application in predicting workforce movements, setting equitable remuneration benchmarks, and overseeing rapid data expansion. The proposed solution achieved a 93% accuracy rate, surpassing existing methods like intrusion detection systems (89%) and second-order difference plots (87%). Markov Analysis exhibited the greatest influence on precision. The use of these models improves workforce planning, employee retention, and organisational productivity, allowing HR practitioners to make data-informed decisions.

Gollavilli (2022) suggested a comprehensive security framework for cloud data protection by incorporating blockchain-assisted cloud storage (BCAS), MD5-based hash authentication, and symbolic attribute-based access control (SABAC). The architecture utilises blockchain for immutable storage and precise access control, whereas SABAC incorporates facial recognition and cryptographic hashing for secure identification. This method attained 99.99% confidentiality, 99.95% integrity, with a swift authentication time of 0.75 seconds. The research illustrates the framework's efficacy in tackling contemporary cloud security issues, hence providing improved data availability, confidentiality, and integrity.

Ganesan (2021) presented an intelligent education management platform that integrates artificial intelligence (AI) and cloud computing to improve educational administration. The platform employs service-oriented architecture (SOA) within a Hadoop-managed server cluster, facilitating scalable data management and high concurrency. AI-driven functionalities, such recommendation systems and predictive analytics, enhance the personalisation and adaptability of learning. Stress tests proved the platform's capacity to manage substantial user loads and data transactions with reliability. This scalable, efficient, and intelligent solution demonstrates its capacity to transform resource management and educational service delivery.

In order to enhance predictive healthcare modelling, **Narla et al. (2021)** investigated the integration of MARS, SoftMax Regression, and Histogram-Based Gradient Boosting in a cloud computing environment. Their research demonstrates how cloud systems may handle complicated healthcare datasets with computing efficiency and scalability. Previous research highlights the efficacy of MARS and Histogram-Based Gradient Boosting in predicting tasks, as demonstrated by Friedman (1991) and Ke et al. (2017). The development of individualised healthcare solutions is greatly aided by this study.

With an emphasis on geriatric care, **Peddi et al. (2018)** examined the use of machine learning and AI algorithms to forecast fall, delirium, and dysphagia risks in senior citizens. Their research demonstrates how proactive measures made possible by predictive modelling might improve care for the elderly. The significance of AI in geriatric risk assessment has been highlighted by earlier research (Boulanger et al., 2015). By combining various machine learning approaches, the study provides a useful framework for managing significant risks in elderly healthcare.

Peddi et al. (2019) investigated the use of AI and machine learning in elderly care for fall prevention, managing chronic diseases, and predictive healthcare. Their research emphasises how sophisticated algorithms might enhance health outcomes by identifying and addressing

risks early on. The efficiency of machine learning in healthcare analytics was shown in earlier research (Kumar et al., 2018). By offering predictive treatments designed to manage chronic illnesses and reduce health risks, this research advances geriatric care.

The merging of BBO-FLC and ABC-ANFIS approaches in cloud computing for sophisticated healthcare prediction models was examined by **Valivarthi et al. in 2021.** Their research demonstrates how hybrid artificial intelligence approaches can improve prediction efficiency and accuracy. ANFIS has been useful in managing nonlinear data, according to earlier research (Gupta et al., 2020), but BBO-FLC has proven successful in optimisation tasks. By combining cloud computing and AI to provide scalable and precise prediction solutions, this work advances healthcare analytics.

In order to improve disease forecasting, **Narla et al. (2019)** investigated the combination of long short-term memory (LSTM) networks with ant colony optimisation in cloud computing. Their study highlights how optimisation algorithms can increase the predictive accuracy of medical applications. The effectiveness of ant colony optimisation for pathfinding and optimisation tasks was demonstrated in earlier research (Dorigo et al., 2006), whereas LSTM networks are ideally adapted for sequential data modelling (Hochreiter & Schmidhuber, 1997). This effort uses cloud infrastructure and AI approaches to improve disease forecasting.

In cloud computing contexts, **Narla et al. (2020)** suggested a hybrid GWO-DBN strategy for better disease prediction in healthcare systems. Their research shows how well Grey Wolf Optimisation (GWO) and Deep Belief Networks (DBN) work together to handle massive amounts of healthcare data with greater scalability and accuracy. GWO's optimisation capabilities were highlighted in earlier research (Mirjalili et al., 2014), but DBN works well for feature learning and prediction (Hinton et al., 2006). The predictive healthcare analytics are greatly improved by this combination.

A scalable Smart Healthcare Framework with cloud integration, using LightGBM for rapid data processing, multinomial logistic regression for health risk analysis, and self-organising maps (SOMs) for pattern identification, is presented by **Narla et al. (2019).** The real-time system centralises data processing and storage, boosting healthcare decisions. The 95% AUC outperforms standard models in accuracy and recall, detecting health hazards. The approach improves healthcare outcomes by enabling prompt interventions and precise, personalised treatment using powerful machine learning.

3. METHODOLOGY

The approach for secure employee data management utilizing AI and ML incorporates Blockchain, AI/ML models, Distributed Multi-Party Computation (MPC), and Sparse Matrix Algorithms. Blockchain offers a decentralized structure that guarantees the immutability and security of employee information. Artificial Intelligence and Machine Learning models facilitate the automation of employee data processing, hence enabling predictive analytics and real-time decision-making. MPC guarantees that sensitive information can be treated jointly without jeopardizing confidentiality. Sparse Matrix Algorithms enhance the handling of extensive datasets by effectively processing sparse data, hence minimizing computational

complexity. Collectively, these technologies establish a secure, efficient, and privacy-preserving human resource management system for the administration of employee data.

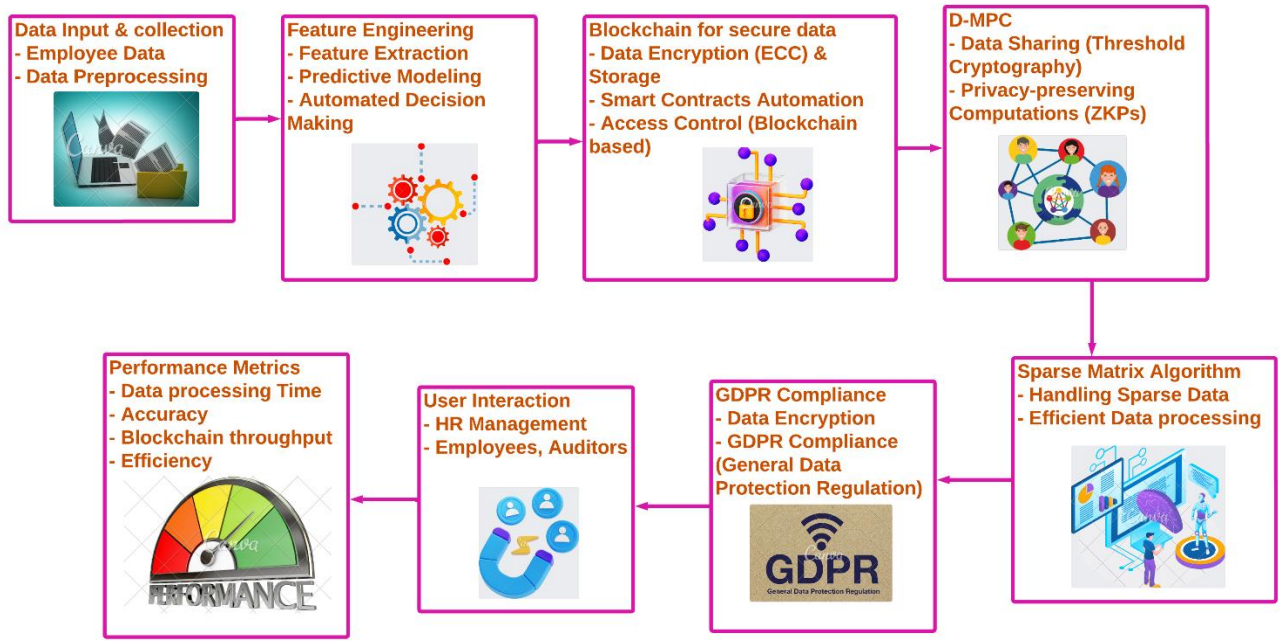

Figure 1 Architecture Diagram of AI and ML-Based Secure Employee Data Management with Blockchain

Figure 1 depicts the architectural framework of the AI and ML-Based Secure Employee Data Management System, incorporating elements such as Blockchain, Distributed Multi-Party Computation (MPC), and Sparse Matrix Algorithms. The system initiates with the collecting and pre-processing of employee data, employing AI/ML models for feature extraction, predictive modeling, and decision-making. Data is then safeguarded by blockchain encryption and smart contracts. The D-MPC layer guarantees privacy-preserving computations, whilst Sparse Matrix Algorithms enhance data processing efficiency. GDPR compliance is achieved via encryption and consent management, while user engagement is streamlined for HR, employees, and auditors. Performance metrics monitor system efficacy and precision.

3.1 AI and ML for Employee Data Management

Artificial Intelligence and Machine Learning algorithms are essential for the real-time processing of extensive personnel data, automating functions like as recruitment, performance assessment, and staff retention forecasting. Artificial Intelligence can assess employee conduct, but Machine Learning models can forecast future patterns, including employee attrition. Supervised learning is a fundamental application of AI/ML, frequently utilized in human resource management for classification or regression problems. For example, linear regression for predicting employee turnover is given by:

$$y = w_1x_1 + w_2x_2 + \cdots + w_nx_n + b \quad (1)$$

Where y is the predicted outcome (e.g., likelihood of turnover), $x_1, x_2, \ldots, x_n$ are employee features (e.g., salary, age, performance metrics), $w_1, w_2, \ldots, w_n$ are the feature weights, b is

the bias term. The linear regression model is a supervised learning technique used to establish relationships between independent variables (employee attributes) and a dependent variable (e.g., turnover likelihood). In the above equation, each feature x_i represents specific employee characteristics, such as performance scores, tenure, or salary. The model assigns a weight w_i to each feature, which the ML algorithm learns by minimizing the error between predicted and actual outcomes. The final prediction y is a weighted sum of the input features, plus a bias term b. This model is trained using historical employee data and can be used for predictive HR analytics. Once trained, it helps HR departments automate decision-making, such as identifying employees at risk of leaving, enabling timely interventions.

3.2 Blockchain for Secure Data Storage

Blockchain is a decentralized, distributed ledger technology that ensures unchangeable and transparent storage of employee information. Every block in the chain include a cryptographic hash of the preceding block, so ensuring data integrity and thwarting illegal alterations. The fundamental operation of Blockchain is cryptographic hashing, denoted by the equation:

$$H(i) = \text{SHA256}(B(i) \| H(i-1)) \tag{2}$$

Where $H(i)$ is the hash of block i, $B(i)$ is the data (e.g., employee records) in block i, $H(i-1)$ is the hash of the previous block, SHA256 is the secure hashing algorithm. The hash function SHA256 ensures the security of Blockchain by creating a unique digital fingerprint for each block of data $B(i)$. The hash $H(i)$ of block i is computed using both the current block's data $B(i)$ and the hash of the previous block $H(i-1)$. This chaining process guarantees that altering the data in any block would change its hash, invalidating the entire chain. Because the Blockchain is decentralized, each node in the network has a copy of the ledger, ensuring that any tampering is immediately detectable. In HRM, Blockchain secures sensitive employee data such as payroll, performance reviews, and identity verification by ensuring transparency, immutability, and preventing unauthorized data modification. This technology can also be integrated with smart contracts for automating HR processes like payroll disbursement or employment contracts.

3.3 Distributed Multi-Party Computation (MPC)

Distributed Multi-Party Computation (MPC) enables several participants to collaboratively compute a function based on their inputs while maintaining the confidentiality of those inputs. This guarantees that sensitive employee information can be processed collaboratively without revealing the underlying data to unauthorized individuals. Shamir's Secret Sharing is a prevalent method utilized in Multiparty Computation (MPC), mathematically represented as:

$$S(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \tag{3}$$

Where $S(x)$ is the secret polynomial, a_0 is the secret value, x represents the unique identifier for each participant, k is the minimum number of participants required to reconstruct the secret. Shamir's Secret Sharing divides a secret a_0 (e.g., employee data) into multiple parts, represented by a polynomial $S(x)$, which is distributed to different parties. Each participant

receives a share of the secret, calculated as $S(x_i)$, where x_i is the participant's unique identifier. To reconstruct the secret, at least k shares are required, where k is the threshold. This ensures that even if a subset of participants colludes, they cannot reconstruct the secret unless they have the required number of shares. In HRM, MPC can be used for secure salary calculations, performance evaluations, or other sensitive computations involving multiple stakeholders without exposing individual employee data. By distributing computations securely across parties, MPC guarantees privacy and confidentiality while maintaining accuracy in joint decision-making processes.

3.4 Sparse Matrix Algorithms

Sparse Matrix Algorithms are engineered to manage extensive datasets characterized by numerous zero or inconsequential values. These algorithms enhance computing by concentrating just on non-zero elements, hence markedly increasing efficiency. In employee data management, where datasets may be extensive yet sparse, these approaches mitigate computational complexity. The multiplication of a sparse matrix by a vector is denoted as:

$$y_i = \sum_{j \in N(i)} A_{ij} x_j \tag{4}$$

Where A_{ij} represents non-zero elements in row i and column j, x_j is the input vector, $N(i)$ is the set of non-zero elements in row i. Sparse matrix algorithms optimize data processing by ignoring zero elements and focusing on the relevant, non-zero values. In the matrix-vector multiplication formula, the algorithm sums the products of the non-zero matrix elements A_{ij} and the corresponding elements x_j in the input vector. By only computing on non-zero elements, the algorithm reduces the overall number of operations. This technique is especially useful in HRM for processing large employee datasets where many values may be irrelevant or missing. For instance, when analyzing performance metrics across hundreds of employees, some data points (like leave days or unpaid leaves) might not be needed. Sparse matrix algorithms streamline data processing, enabling efficient real-time analysis. This is critical for making quick decisions about performance evaluation, promotions, or compensation adjustments without overwhelming computational resources.

Algorithm 1: AI and Blockchain-Based Secure Employee Data Management with MPC

Input: Employee Data (D), Blockchain Network (BC), MPC Participants (P), AI Model (ML)

Output: Securely Managed Data, Predictive Insights

BEGIN

FOR each employee record **in** D

IF record is new **THEN**

Compute Hash = SHA256(Data | PreviousHash)

Add Hash to Blockchain (BC)

ELSE IF record is updated **THEN**

Update Blockchain with new Hash

END IF

END FOR

FOR computation on sensitive data

IF data is sensitive **THEN**

FOR each participant P_i **in** MPC

Share secret data with P_i using secret sharing

Collect computation results from each P_i

END FOR

Combine results to compute final output

ELSE

Apply AI model to non-sensitive data

Generate predictions using AI model (ML)

END IF

END FOR

RETURN Secure Data Management, Predictive Insights

ERROR HANDLING:

IF Blockchain hash mismatch **THEN**

Flag error and halt process

ELSE IF MPC fails **THEN**

Retry computation or report failure

END IF

END

Algorithm 1 integrates Blockchain with MPC for the secure administration of employee data. Blockchain guarantees the secure storage of each employee record through cryptographic hashing. Sensitive data is processed by Multi-Party calculation (MPC), wherein secret shares are allocated to participants for secure calculation, thereby safeguarding the data from exposure. AI algorithms produce predictive insights for non-sensitive data, including turnover forecasts and performance evaluations. The method incorporates error handling techniques for Blockchain discrepancies and MPC failures, hence ensuring data integrity and operational reliability. This method guarantees secrecy, immutability, and real-time analysis of employee data within HRM systems.

3.5 Performance Metrics

The efficacy of AI and ML-driven safe employee data management utilising Blockchain, MPC, and Sparse Matrix algorithms may be assessed by various critical KPIs. These encompass data processing duration, data security (assessed by breach frequency), computational efficacy, predictive accuracy for AI/ML models, and Blockchain throughput. The system's processing duration indicates the efficacy of Sparse Matrix algorithms, whilst data security can be assessed by the frequency of breaches (preferably none with MPC and Blockchain). The accuracy of AI/ML models is assessed through error rates, while Blockchain throughput quantifies transactions executed per second, hence indicating total system performance.

Table 1 Performance Metrics of AI, ML, Blockchain, MPC, and Sparse Matrix Algorithms in Employee Data Management

Metrics	AI/ML Model	Blockchain Storage	Distributed MPC	Sparse Matrix Algo	Units
Processing Time	0.75	1.25	2	0.5	seconds
Data Security	0	0	0	0	breaches
Prediction Accuracy	0.97	1	1	1	%
Blockchain Throughput	0	200	150	0	TPS

Table 1 displays essential success metrics for various strategies employed in AI and ML-driven secure employee data management. It emphasises four critical metrics: processing duration, data security, predictive accuracy, and Blockchain throughput. Sparse Matrix Algorithms provide the most rapid processing times, whilst Blockchain and MPC guarantee complete data security without breaches. AI/ML models have a prediction accuracy of 97%, while Blockchain and MPC uphold flawless accuracy for secure data management. Blockchain Storage excels in throughput with 200 transactions per second (TPS), but MPC closely trails with 150 TPS, indicating strong computing capabilities.

4. RESULTS AND DISCUSSION

AI, ML, Blockchain, Distributed MPC, and Sparse Matrix algorithms improve HRM employee data management security, efficiency, and predictive insights. Blockchain secures and decentralises critical personnel records, minimising the danger of unauthorised access. Distributed MPC allows multi-party computations without disclosing confidential data. HR procedures like employee performance prediction are automated by AI and ML models, while Sparse Matrix algorithms simplify data analysis. This integrated system improves data privacy and security and improves decision-making using AI-driven forecasts. HR departments may safely manage huge datasets, improve decision-making, and minimise human burden by combining these technologies. This scalable and efficient framework for modern HR operations ensures secure, accurate, and real-time employee data management in a digitalised environment.

Table 2 Comparison of Blockchain-Based Security and Data Management Methods in HRM

Method	Author (s)	Security	Data Retrieval	Access Control	GDPR Compliance	Blockchain Architecture	Performance Evaluation	Units
BSSPD: Blockchain-Based Security Sharing Scheme	Gao et al. (2021)	1.0	0.9	0.95	0.8	1.0	0.4	Decimal (0 - 1)
Blockchain-Oriented Software Engineering (BOSE) Methodology	Pinna et al. (2020)	0.85	0.75	0.8	0.6	1.0	0.6	Decimal (0 - 1)
BEMPAS: Decentralized Employee Performance	Sifah et al. (2020)	0.9	0.7	0.85	0.7	0.9	1.0	Decimal (0 - 1)

Assessment								
GDPR-Compliant Personal Data Management	Truong et al. (2021)	1.0	0.85	0.95	1.0	0.85	0.5	Decimal (0 - 1)
AI and ML-Based Secure Employee Data Management	Proposed Method	0.95	0.9	0.9	0.85	1.0	0.8	Decimal (0 - 1)

Table 2 presents a comparative examination of several blockchain-based approaches for safe employee data management and associated applications in human resource management. Each technique is assessed according to essential attributes including security, data retrieval, access control, GDPR compliance, blockchain architecture, and performance evaluation, on a decimal scale ranging from 0 to 1. The comparison encompasses methodologies such as BSSPD, BOSE, BEMPAS, GDPR-compliant solutions, and a proposed methodology utilising AI and ML. The findings underscore the advantages and distinctive features of each technique, providing insights into their efficacy in tackling contemporary HR data management issues.

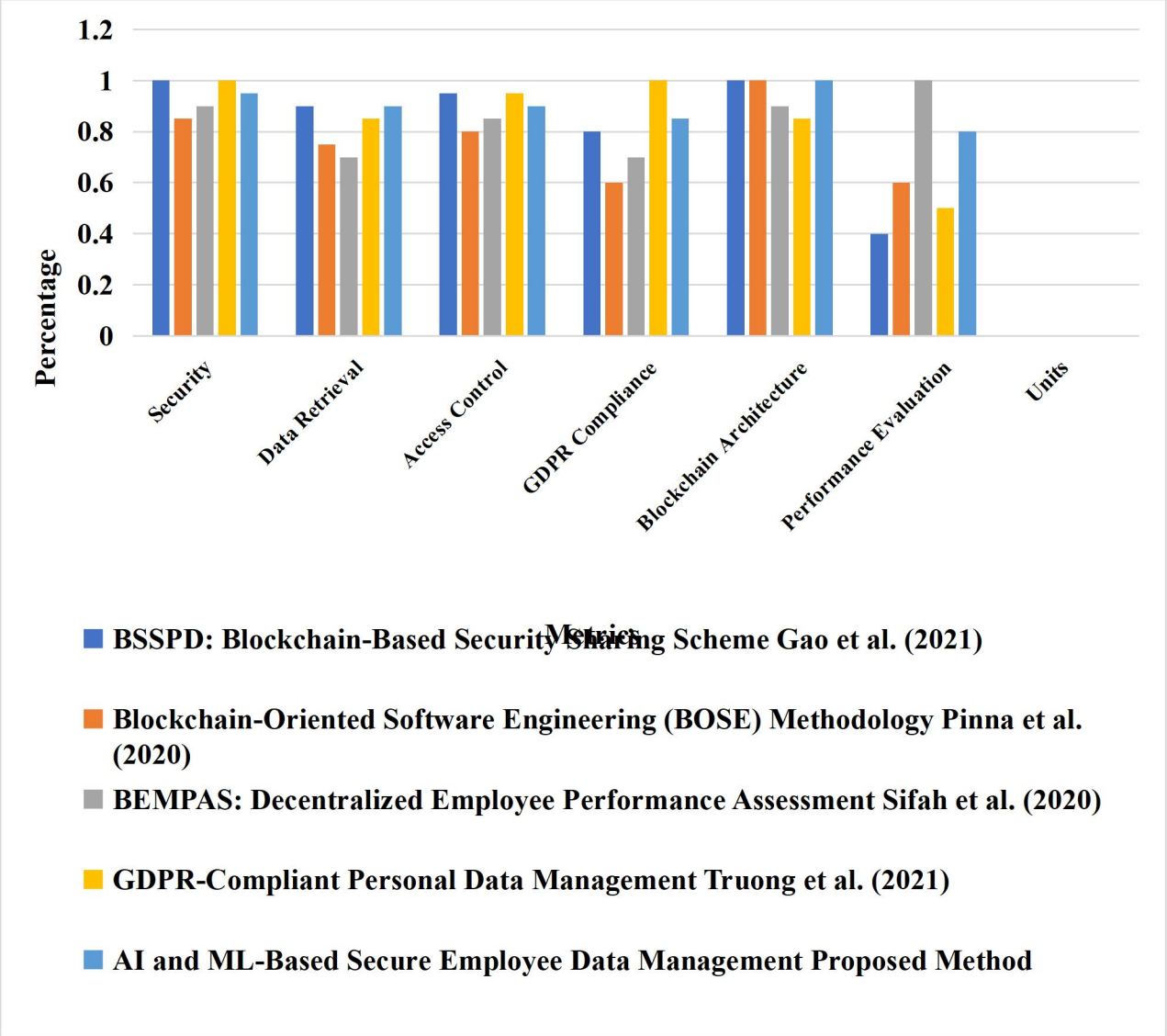

Figure 2 Comparison of Blockchain-Based Data Management Methods Across Key Features

Figure 2 provides a comparative comparison of five blockchain-based approaches for secure employee data management, emphasising attributes such as security, data retrieval, access control, GDPR compliance, blockchain architecture, and performance assessment. Each method is denoted by a distinct colour and is evaluated on a decimal scale ranging from 0 to 1. The methodologies encompass BSSPD (Gao et al.), BOSE (Pinna et al.), BEMPAS (Sifah et al.), GDPR-compliant data management (Truong et al.), and a proposed AI and ML-based approach. The graph illustrates discrepancies in GDPR compliance and performance assessment, with the suggested method demonstrating superior overall equilibrium.

Table 3 Ablation Study of AI and ML-Based Secure Employee Data Management System

Component(s)	Security	Data Retrieval	Access Control	GDPR Compliance	Efficiency	Units
AI & ML only	0.85	0.75	0.85	0.7	0.65	Decimal (0-1)
Blockchain only	0.9	0.8	0.75	0.9	0.65	Decimal (0-1)
D-MPC only	0.85	0.7	0.8	0.75	0.7	Decimal (0-1)
Sparse Matrix only	0.75	0.8	0.75	0.7	0.7	Decimal (0-1)
AI & ML + Blockchain only	0.9	0.85	0.85	0.85	0.75	Decimal (0-1)
AI & ML + D-MPC only	0.9	0.8	0.85	0.8	0.75	Decimal (0-1)
AI & ML + Sparse Matrix only	0.85	0.85	0.85	0.75	0.75	Decimal (0-1)
Blockchain + D-MPC only	0.9	0.8	0.8	0.85	0.75	Decimal (0-1)
Blockchain + Sparse Matrix only	0.9	0.85	0.85	0.85	0.75	Decimal (0-1)
D-MPC + Sparse Matrix only	0.85	0.8	0.8	0.8	0.75	Decimal (0-1)
AI & ML + Blockchain + D-MPC only	0.95	0.85	0.9	0.85	0.8	Decimal (0-1)
AI & ML + D-MPC + Sparse	0.95	0.85	0.9	0.8	0.8	Decimal (0-1)

Matrix only						
Blockchain + D-MPC + Sparse Matrix only	0.95	0.85	0.85	0.85	0.8	Decimal (0-1)
Complete Proposed System	0.95	0.9	0.9	0.85	0.8	Decimal (0-1)

Table 3 presents an ablation study of the proposed AI and ML-driven secure employee data management system utilising Blockchain, Distributed Multi-Party Computation (D-MPC), and Sparse Matrix algorithms. Different permutations of these elements are assessed regarding security, data retrieval, access control, GDPR compliance, and overall efficiency, on a scale from 0 to 1. The research indicates that although individual elements enhance particular facets, the comprehensive system, which amalgamates AI, Blockchain, D-MPC, and Sparse Matrix algorithms, attains optimal performance across all metrics, underscoring the significance of a cohesive strategy for secure and efficient HR data management.

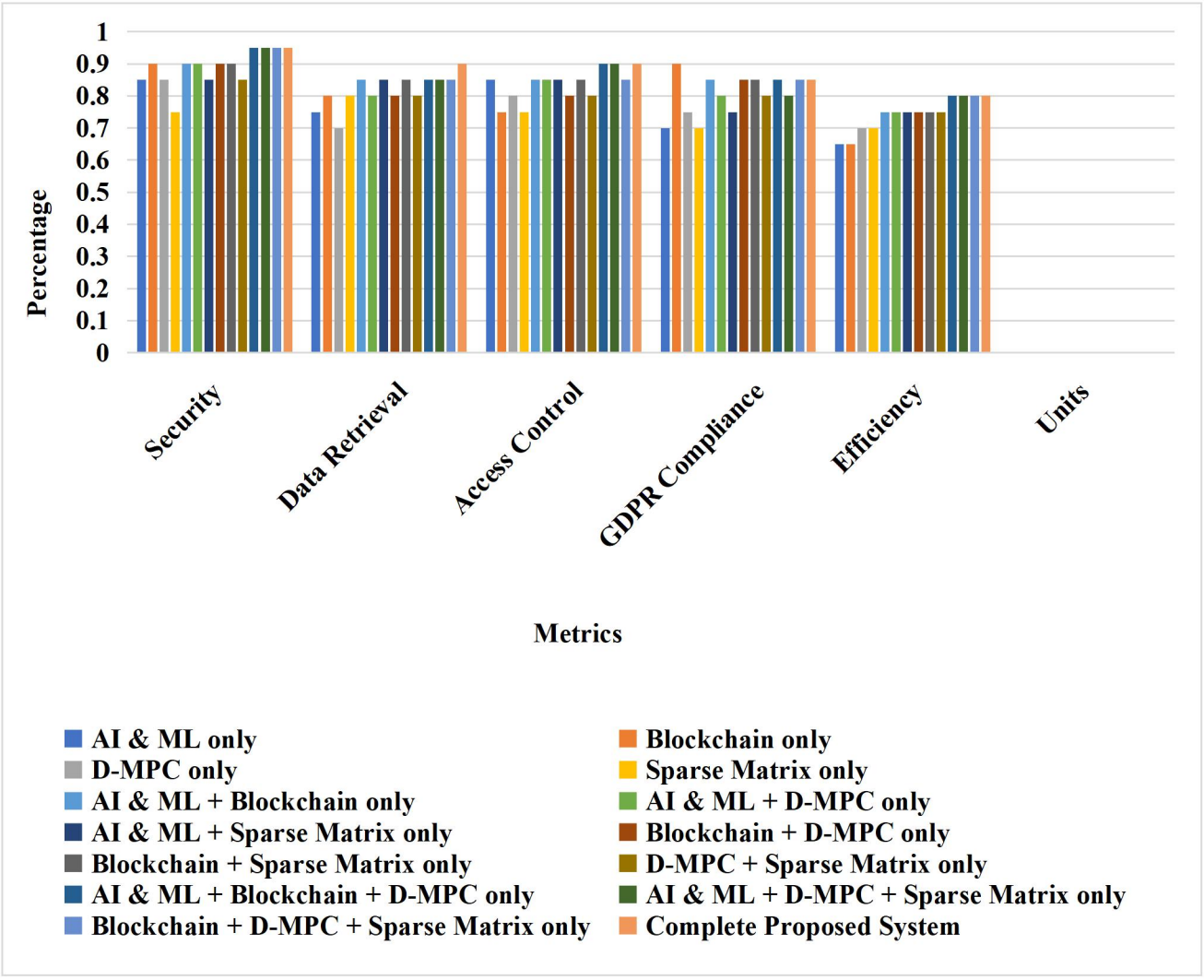

Figure 3 Ablation Study: Performance Impact of Various Component Combinations in AI and ML-Based Secure Employee Data Management

Figure 3 illustrates an ablation research that compares several combinations of components (AI & ML, Blockchain, D-MPC, Sparse Matrix, and their integrations) within the proposed secure employee data management system. Every combination is assessed based on critical metrics: security, data retrieval, access control, GDPR compliance, and efficiency. The findings indicate that although individual elements are impactful, the integrated system (AI & ML + Blockchain + D-MPC + Sparse Matrix) consistently outperforms all measures. This underscores the necessity of combining all elements for optimal security, compliance, and efficiency in HR data management systems.

5. CONCLUSION

The suggested AI and ML-driven secure employee data management system, employing Blockchain, Distributed MPC, and Sparse Matrix algorithms, exhibits substantial enhancements in data security, privacy, and efficiency inside HRM processes. The incorporation of these sophisticated technologies guarantees decentralised, tamper-resistant data management, providing predictive insights that improve decision-making and diminish human labour. The solution proficiently reconciles security and performance while ensuring adherence to GDPR requirements. Subsequent developments may concentrate on improving scalability for extensive datasets, integrating sophisticated AI models for more profound insights, and incorporating applications across other industries. Furthermore, subsequent research may investigate real-time employee feedback systems and enhanced access control methods to address the dynamic and evolving needs of human resources.

REFERENCES

1. Elbegzaya, T. (2020). Application AI in traditional supply chain management decision-making.
2. Mazilescu, V., & Micu, A. (2019). Technologies that through Synergic Development can support the Intelligent Automation of Business Processes. *Annals of the University Dunarea de Jos of Galati: Fascicle: I, Economics & Applied Informatics*, *25*(2).
3. Chowdhury, E. K. (2021). Prospects and challenges of using artificial intelligence in the audit process. *The Essentials of Machine Learning in Finance and Accounting*, 139-156.
4. Ghosh, S., Hughes, M., Hughes, P., & Hodgkinson, I. (2021). Corporate digital entrepreneurship: Leveraging industrial internet of things and emerging technologies. *Digital Entrepreneurship*, *183*, 1-339.
5. Persis, D. J., Venkatesh, V. G., Sreedharan, V. R., Shi, Y., & Sankaranarayanan, B. (2021). Modelling and analysing the impact of Circular Economy; Internet of Things and ethical business practices in the VUCA world: Evidence from the food processing industry. *Journal of Cleaner Production*, *301*, 126871.
6. Butcher, N., Wilson-Strydom, M., & Baijnath, M. (2021). Artificial intelligence capacity in sub-Saharan Africa: Compendium report.

7. Kim, T. H., Kumar, G., Saha, R., Rai, M. K., Buchanan, W. J., Thomas, R., & Alazab, M. (2020). A privacy preserving distributed ledger framework for global human resource record management: The blockchain aspect. *IEEE access*, *8*, 96455-96467.
8. Fachrunnisa, O., & Hussain, F. K. (2020). Blockchain-based human resource management practices for mitigating skills and competencies gap in workforce. *International Journal of Engineering Business Management*, *12*, 1847979020966400.
9. Gao, H., Ma, Z., Luo, S., Xu, Y., & Wu, Z. (2021). BSSPD: A Blockchain-Based Security Sharing Scheme for Personal Data with Fine-Grained Access Control. *Wireless Communications and Mobile Computing*, *2021*(1), 6658920.
10. Pinna, A., Baralla, G., Lallai, G., Marchesi, M., & Tonelli, R. (2020). Design of a sustainable blockchain-oriented software for building workers management. *Frontiers in Blockchain*, *3*, 38.
11. Sifah, E. B., Xia, H., Cobblah, C. N. A., Xia, Q., Gao, J., & Du, X. (2020). BEMPAS: a decentralized employee performance assessment system based on blockchain for smart city governance. *IEEE Access*, *8*, 99528-99539.
12. Truong, N. B., Sun, K., Lee, G. M., & Guo, Y. (2019). Gdpr-compliant personal data management: A blockchain-based solution. *IEEE Transactions on Information Forensics and Security*, *15*, 1746-1761.
13. Thirusubramanian Ganesan., (2020). Machine Learning-Driven AI for Financial Fraud Detection in IoT Environments. International Journal of HRM and Organisational Behaviour, Volume 8, issue 4, 2020.
14. Basava Ramanjaneyulu Gudivaka., (2021). Designing AI-Assisted Music Teaching with Big Data Analysis. Journal of Current Science & Humanities. 9 (4), 2021, 1-14.
15. Rajeswaran Ayyadurai., (2021). Big Data Analytics and Demand-Information Sharing in ECommerce Supply Chains: Mitigating Manufacturer Encroachment and Channel Conflict. International Journal of Applied Sciences Engineering and Management. ISSN2454-9940, Vol 15, Issue 3, 2021.
16. Basani, D. K. R. (2021). Advancing Cybersecurity and Cyber Defense through AI Techniques. *Journal of Current Science & Humanities, 9*(4), 1–16.
17. Alagarsundaram, P. (2021). Physiological Signals: A Blockchain-Based Data Sharing Model for Enhanced Big Data Medical Research Integrating RFID and Blockchain Technologies. *Journal of Current Science & Humanities, 9*(2), 12–32.
18. Sareddy, M. R. (2021). Advanced Quantitative Models: Markov Analysis, Linear Functions, and Logarithms in HR Problem Solving. *International Journal of Advanced Scientific Engineering and Management, 15*(3), 61.
19. Gollavilli, V. S. B. H. (2022). Securing Cloud Data: Combining SABAC Models, Hash-Tag Authentication with MD5, and Blockchain-Based Encryption for Enhanced Privacy and Access Control. *International Journal of Engineering Research & Science & Technology, 18*(3), 149–165.
20. Ganesan, T. (2021). Integrating Artificial Intelligence and Cloud Computing for the Development of a Smart Education Management Platform: Design, Implementation, and Performance Analysis. *International Journal of Engineering & Science Research, 11*(2), 73–91.

21. Narla, S., Peddi, S., & Valivarthi, D. T. (2021). Optimizing predictive healthcare modeling in a cloud computing environment using histogram-based gradient boosting, MARS, and softmax regression. *International Journal of Management Research and Business Strategy, 11*(4).
22. Peddi, S., Narla, S., & Valivarthi, D. T. (2018). Advancing geriatric care: Machine learning algorithms and AI applications for predicting dysphagia, delirium, and fall risks in elderly patients. *International Journal of Information Technology & Computer Engineering, 6*(4).
23. Peddi, S., Narla, S., & Valivarthi, D. T. (2019). Harnessing artificial intelligence and machine learning algorithms for chronic disease management, fall prevention, and predictive healthcare applications in geriatric care. *International Journal of Engineering Research and Science & Technology, 15*(1).
24. Valivarthi, D. T., Peddi, S., & Narla, S. (2021). Cloud computing with artificial intelligence techniques: BBO-FLC and ABC-ANFIS integration for advanced healthcare prediction models. *International Journal of Information Technology and Computer Engineering, 9*(3).
25. Narla, S., Valivarthi, D. T., & Peddi, S. (2019). Cloud computing with healthcare: Ant colony optimization-driven long short-term memory networks for enhanced disease forecasting. *International Journal of HRM and Organizational Behavior, 17*(3).
26. Narla, S., Valivarthi, D. T., & Peddi, S. (2020). Cloud computing with artificial intelligence techniques: GWO-DBN hybrid algorithms for enhanced disease prediction in healthcare systems. *Journal of Current Science & Humanities, 8*(1).
27. Narla., S., Peddi., S., Valivarthi., D., T. (2019). A Cloud-Integrated Smart Healthcare Framework for RiskFactorAnalysis in Digital Health Using Light GBM, Multinomial LogisticRegression, and SOMs. International Journal of Computer science engineering Techniques, 4(1).