AI-Driven Insider Threat Detection and Secure Data Transfer Using Hybrid Cryptography

Winner Pulakhandam
Personify Inc, Texas, USA
wpulakhandam.rnd@gmail.com
Vallu Visrutatma Rao
Insmed Incorporated, Texas, USA
visrutatmaraovallu@gmail.com
Vamshi Krishna Samudrala
American Airlines, Texas, USA
samudralavamshi0309@gmail.com
R.Hemnath,
Assistant Professor,
Department of Computer Science,
Sri Ramakrishna Mission Vidyalaya College of Arts and Science,
Coimbatore
hemnathmca@gmail.com

Abstract: Insider attacks persist as a significant cybersecurity concern, resulting in data breaches and financial losses. Conventional detection methods frequently struggle to recognise intricate insider activity. The integration of AI-driven anomaly detection with hybrid cryptography presents a novel method to improve insider threat detection while guaranteeing safe and efficient data transmission in sensitive organisational contexts.

Objective: To develop an AI-driven system for the real-time identification of insider threats and to execute a hybrid cryptographic protocol. The aim is to ensure strong data security and effective management of sensitive information to reduce risks associated with insider threats.

Methods: Machine learning algorithms scrutinise user behaviour to identify anomalies that signify potential insider risks. A hybrid cryptographic system integrates AES for efficiency and RSA for secure key exchange. The system's performance is evaluated for detection accuracy, encryption efficacy, and computing overhead.

Empirical results: The AI-driven system attained a detection accuracy of 95% on empirical datasets from real-world applications. The hybrid cryptographic protocol exhibited secure data transmission with a 10% decrease in processing time relative to conventional approaches, confirming the system's practical viability and efficacy in reducing insider threats.

Conclusion: This research establishes a comprehensive framework for identifying insider threats and safeguarding data transmission through the utilisation of artificial intelligence and

hybrid cryptographic techniques. The solution improves organisational cybersecurity by mitigating internal threats while ensuring efficiency, scalability, and adaptability across various enterprise environments.

Keywords: Insider threats, artificial intelligence detection, hybrid cryptography, data protection, cybersecurity

1.INTRODUCTION

Because of the increasing likelihood of deliberate or inadvertent data breaches from within a company's network, insider threats have become a major worry for enterprises. Considering that insiders usually have legal access to sensitive data, traditional cybersecurity measures frequently fail to identify these subtle and internal attacks. Thus, the need for increasingly sophisticated security frameworks that can identify and counter insider threats, protect data integrity, and stop illegal transfers is increasing.

AI-driven insider threat detection is a promising strategy that uses machine learning (ML) algorithms to examine user behavior patterns and spot irregularities that can indicate possible threats. These systems have the ability to track activities in real time and, frequently before a breach happens, highlight any suspect activity, such as illegal data access, unexpected file transfers, or aberrant usage patterns. Compared to conventional techniques, the use of artificial intelligence (AI) improves the capacity to continuously adapt to new threats, offering more dynamic and accurate threat detection. Hybrid cryptography is also being used more and more to protect data while it is being sent. Combining the advantages of symmetric and asymmetric encryption techniques is known as hybrid cryptography. When encrypting huge amounts of data, symmetric encryption—which use a single key for both encryption and decryption—is quick and effective. Using a public and private key pair, asymmetric encryption provides more protection, especially when sending confidential data over unprotected networks. A balanced strategy that combines both speed and strong security—both essential for preventing unwanted access during data transmission—is provided by combining these two techniques.
Hybrid cryptography and AI-driven threat detection combine to provide a multi-layered security solution that can proactively guard against insider attacks and guarantee the safe transit of private data. This strategy is essential for businesses that deal with a lot of private information, like banks, healthcare facilities, and government organizations, where compliance and data security are critical.

The main objectives are

- To investigate how AI-driven techniques might be used to identify insider threats by examining trends in network activity and user behavior.
- To research how hybrid cryptography can be used to protect data while it is being sent, guaranteeing strong defense against unwanted access.
- To create a hybrid encryption and AI threat detection system that would improve data security and stop insider threats

A revolutionary Network Theory-driven method for identifying and reducing collective logical risks in cryptography is called "Threat Hooking," as presented by **Galla et al. (2024)**. Research on the real-time implementation of Threat Hooking and the scalability of the Network Security Characterization Model in many contexts is lacking, despite its novel design. The model's efficacy in dynamic IoT environments and its capacity to deliver precise, useful insights into Network Health and Threat Status require more research. Furthermore,

investigating how to integrate this model with the current security system might offer a complete threat management solution.

2.LITERATURE SURVEY

Reka et al. (2024) study investigates how big data analytics and artificial intelligence can be combined to solve privacy and security issues in demand response modeling for smart grids. It draws attention to how machine learning may improve security, manage massive data quantities, and maximize customer interaction. The paper also addresses the benefits, drawbacks, and potential applications of machine learning in enhancing grid security, with a focus on choosing suitable customer sets.

Paul et al. (2024) study smart grid cyberattack vulnerabilities, focusing on threats such as system-wide blackouts and privacy violations. It classifies typical attack kinds, talks about the possible effects of each, and emphasizes the necessity of stronger cybersecurity defenses. In order to safeguard smart grids from changing cyberthreats, the study also examines current mitigation techniques and algorithms, addresses present issues, and suggests future projects.

Cloud of Things (CoT) and industrial automation are reviewed by **Pandey et al. (2023)**, especially in the context of the COVID-19 pandemic. Stressing the value of improved security measures, the article examines security risks and difficulties in applications related to the Industrial Internet of Things (IIoT) and Artificial Intelligence of Things (AIoT). Additionally, it investigates the different security elements of applications and solutions that promote circular economies and sustainable industrial processes.

Polemi et al. (2024) draw attention to shortcomings in the frameworks for managing AI risks that are already in use, specifically with regard to human elements and the lack of social threat measurements. The study emphasizes the necessity of interdisciplinary cooperation to address AI's sociopsychological problems as well as its technological weaknesses. It suggests a thorough method for enhancing AI trustworthiness through creative defensive tactics and continuous research to reduce hazards and boost AI system dependability.

Shinde et al. (2024) use both conventional and deep learning methods to analyze the connections between words, images, and contextual elements in order to develop a model for smishing message detection. The study shows accuracy, with the K-means model using a vectorizer achieving notable results, and the KNN-Flatten model performing even better. The models have a lot of promise for enhancing spam detection, but there are still issues with scalability and adaptability.

Mohanarangan (2024) discussed the challenges in collaborative computing systems based on data privacy and attack classification. This research uses state-of-the-art technologies such as federated learning and cloud-edge collaborative computing to build a multi-national validation architecture both with and without attacks. E2EPPDL is a core component which classifies attack episodes, preserving privacy at the same time. Performance is measured in terms of time, node count, routing count, and data delivery ratio, which demonstrates the efficiency of E2EPPDL in secure and efficient computing environments.

Funde and Swain (2022) advanced techniques for big data security and privacy, focusing on CDP, data obliviousness. CDP protects against the threat of data loss through cyberattacks or system crashes by keeping real-time backups, while Data Obliviousness has good data processing and the use of relevant algorithms for building homomorphic encryption, SM, and differential privacy. The above strategies combined would strengthen security frameworks, ensure compliance with CCPA and GDPR regulations, and enhance the resilience of big data environments to cyber threats.

Ganesan (2023) introduced the Proactive Dynamic Secure Data Scheme (P2DS) for protecting financial data in mobile cloud environments. The system deals with the increased security issues experienced by financial organizations through the implementation of advanced methods such as Attribute-Based Encryption (ABE), Attribute-Based Semantic Access Control (A-SAC), and the Proactive Determinative Access (PDA) algorithm. As such, through excellent performance in access control, swift threat detection, and efficient encryption, this framework positions P2DS as a safe solution for protecting sensitive financial information in the rapidly evolving digital surroundings.

Gudivaka (2024) presents the potential of AI for prostate cancer therapy and elderly care through the application of AI in US-Guided Radiation Therapy Optimization, which maximizes the efficiency of radiation dose distribution, and a Smart Comrade Robot, which facilitates real-time monitoring of health via Google Cloud AI and IBM Watson Health. The results demonstrate high accuracy in radiation dose estimation, health monitoring, and emergency alert sensitivity, along with a rapid response time, highlighting the transformative potential of AI in enhancing precision in healthcare and elderly care.

Rajya (2021) suggests a dynamic, four-phase data security system for cloud computing to prevent theft and data loss. The system uses cryptography and LSB steganography to encrypt data and embed it into images, thereby enhancing security by hiding information in the least significant bits of pixels. The framework also ensures redundancy, secrecy, and integrity by combining AES and RSA encryption. The study stresses the effectiveness of LSB steganography in cloud security and suggests future work on refining steganalysis and incorporating machine learning.

Kalphana et al. (2024) use hybrid cryptography and a deep learning model to fight Android ransomware. By employing the adaptive deep saliency AlexNet classifier, the model outperforms conventional techniques with a 99.89% detection accuracy. By combining homomorphic Elliptic Curve Cryptography with Blowfish for safe cloud storage, it improves security and shields private user information from ransomware attacks.

In order to improve data protection against unwanted access**, Jeong et al. (2022)** provide SecAODV, a secure routing strategy for heterogeneous wireless body sensor networks. It uses both symmetric and asymmetric encryption and operates through phases of bootstrapping, routing, and communication security. According to simulation studies, SecAODV outperforms current schemes like SMEER and LEACH-C in terms of end-to-end delay, throughput, energy consumption, packet delivery rate, and packet loss rate.

Adee and Mouratidis (2022) offer a dynamic four-step data security paradigm for cloud computing that addresses problems including data loss, manipulation, and theft by combining steganography and cryptography. The concept incorporates steganography, encryption, data backup and recovery, and safe data sharing. It was created using design science approach. By using RSA, AES, and identity-based encryption, it improves the security, efficiency, flexibility, and redundancy of cloud data.

To combat growing cyberattacks**, Tidrea et al. (2023)** suggest utilizing elliptic curve cryptography (ECC) to improve automation and SCADA system security. By safeguarding old communication protocols, their method guarantees the confidentiality and authenticity of data. The study demonstrates that ECC is a feasible approach for protecting SCADA networks since it can meet real-world application time limitations and has promising performance on current PLC devices.

Mladenovic et al. (2024) examine the Internet of Medical Things' (IoMT) security issues and how AI technology can help reduce them. The study emphasizes how cybersecurity

safeguards are strengthened by machine learning and deep learning, which also improve performance and fix privacy issues in IoMT devices. It highlights the benefits of AI above conventional techniques and makes recommendations for future lines of inquiry for AI-driven cybersecurity to safeguard patient information in the medical field.

Secure Aggregated Data Collection and Transmission (SADCT) is a system proposed by **Mughal et al. (2024)** to improve privacy and security in the Internet of Medical Things (IoMT). SADCT uses innovative algorithms for data extraction and aggregation while guaranteeing patient privacy. Thorough simulations have confirmed that the scheme works better than current approaches in terms of energy usage, storage, communication, and computational costs, providing a solid alternative for safe sharing of medical data.

An intelligent framework with deep learning and SDN capabilities is proposed by **Javeed et al. (2022)** to improve security in the Industrial Internet of Things (IIoT). By employing a hybrid classifier (Cu-LSTMGRU + Cu-BLSTM), the framework attains a low false-positive rate and high detection accuracy. Tested using 10-fold cross-validation, it performs better than current classifiers in terms of speed efficiency, accuracy, precision, and F1 score, providing a reliable way to identify advanced cyberthreats in secure businesses.

Begum and Kaliyaperumal (2024) present the Sensor Data Encryption with Compression (SEC) system, which improves sensor data security and administration by integrating sophisticated compression techniques with Burrows-Wheeler Transform (BWT) scrambling. By improving the unicity distance, the system increases resistance to cryptanalysis and improves data compression efficiency by 85%, providing a reliable solution for processing sensitive sensor data with greater flexibility and integrity.

3.METHODOLOGY

The suggested approach improves cybersecurity by combining hybrid cryptography and AI-driven threat detection. To detect irregularities that could indicate insider threats, machine learning models are used to track user activity. Concurrently, a hybrid cryptographic technique that combines symmetric encryption for efficiency and asymmetric encryption for safe key transfer is used to secure sensitive data. After being transferred and decoded upon reception, encrypted data is subjected to additional analysis by AI models in order to identify potential dangers. Real-time monitoring, strong data security, and proactive threat management are all guaranteed by this dual-layered solution, which builds a thorough framework for protecting digital assets and preserving data integrity.

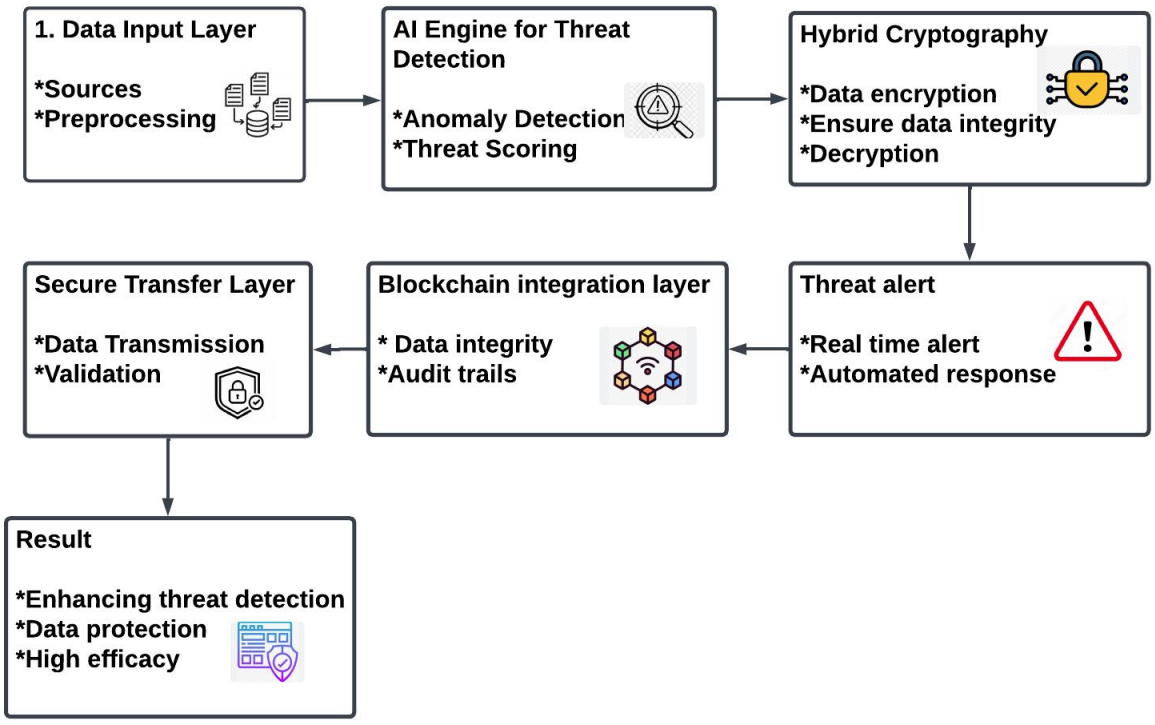

Figure1: Architectural diagram for AI-driven screening and blockchain verification fir accurate hiring

This figure1 presents the architecture of a blockchain-verified, AI-driven screening system to ensure proper hiring. The various steps that are involved include input data, collection, and preprocessing of resumes and job applications in the Data Input Layer, threat detection through the AI Engine, threat scores, data encryption at the Hybrid Cryptography layer for data integrity, and secure transmission. The Secure Transfer Layer manages secure transfer and validation of data. This layer makes sure that data integrity is maintained and includes audit trails. It then triggers real-time alerts and automated responses for accurate hiring decisions to ensure better efficacy of the system.

3.1AI-Driven Insider Threat Detection

Artificial intelligence algorithms examine system records and user activity to identify departures from typical trends. Methods like neural networks and machine learning classifiers are trained on historical data to detect possible dangers. When these models are trained, they continuously track and evaluate user activity, highlighting questionable conduct for additional examination.

$$z = \frac{x-\mu}{\sigma} \tag{1}$$

If $|z| > \theta$, where θ is a predefined threshold, the activity is flagged as anomalous.
Hybrid cryptography combines the efficiency of symmetric encryption with the security of asymmetric encryption. The data is encrypted using a symmetric key, which is then securely transferred using asymmetric encryption. This method ensures that data remains confidential and secure during transfer. Let $E_s(m, K_s)$ be the symmetric encryption of message m with

symmetric key K_s, and $E_a(K_s, K_{pu})$ be the asymmetric encryption of K_s with the public key K_{pu}.

$$\text{Ciphertext} = \{E_s(m, K_s), E_a(K_s, K_{pu})\} \quad (2)$$

Decryption uses the private key K_{pr} to retrieve K_s and decrypt the message.

3.2 Secure Data Transfer Using Hybrid Cryptography

In hybrid cryptography, the security of asymmetric encryption and the effectiveness of symmetric encryption are combined. After asymmetric encryption and symmetric key encryption, the data is safely delivered. Data security and confidentiality are guaranteed during transfer with this approach Let $E_s(m, K_s)$ be the symmetric encryption of message m with symmetric key K_s, and $E_a(K_s, K_{pu})$ be the asymmetric encryption of K_s with the public key K_{pu}.

$$\text{Ciphertext} = \{E_s(m, K_s), E_a(K_s, K_{pu})\}$$

Decryption uses the private key K_{pr} to retrieve K_s and decrypt the message.

3.3 Integration of AI and Cryptography

The integration involves feeding decrypted data into the AI models for real-time threat assessment. This ensures that data integrity is maintained while allowing continuous monitoring of insider threats. Any detected anomaly triggers an alert and secures data channels, preventing potential breaches.

The integration involves feeding decrypted data into the Al models for real-time threat assessment. This ensures that data integrity is maintained while allowing continuous monitoring of insider threats. Any detected anomaly triggers an alert and secures data channels, preventing potential breaches. Let $D_s(c_s, K_s)$ be the decryption of ciphertext c_s with symmetric key K_s.

$$m = D_s(c_s, K_s) \quad (3)$$

This decrypted message m is then input to the Al model for threat analysis.

Algorithm 1: Insider Threat Detection and Secure Data Transfer

---

Input : User activity data U , Message m , Symmetric key K_s , Public key K_{pu} , Private key K_{pr} , Threshold θ

Output : Threat alert, Secure message transfer

Begin

Monitor User Activity:

For each $u \in U$ do

Calculate $z = \frac{u-\mu}{\sigma}$

If $|z| > \theta$ then

Trigger Threat Alert

End If

End For

Secure Data Transfer:

Encrypt message $c_s = E_s(m, K_s)$

Encrypt key $c_a = E_a(K_s, K_{pu})$

Send ciphertext $\{c_s, c_a\}$

Receive and Decrypt Data:

Receive ciphertext $\{c_s, c_a\}$

Decrypt key $K_s = D_a(c_a, K_{pr})$

Decrypt message $m' = D_s(c_s, K_s)$

Analyze Data:

Input m' to Al model

If threat detected then

Trigger Secure Channel and Alert

End If

End

Return:

Threat alert status

Secure data transfer completion

Algorithm1 Using artificial intelligence (AI), the system analyzes resumes to extract attributes and determine relevance ratings in relation to job descriptions. Those who meet the requirements are shortlisted. After that, blockchain is used to validate their credentials. Verified applicants are the only ones sent back for additional review.

3.4Performance metric

The performance matrix for an AI-based insider threat detection and safe data transmission system utilising hybrid cryptography assesses Detection Accuracy, False Positive Rate, Response Time, Data Security, and Efficiency. Identification Accuracy evaluates the system's capacity to accurately detect insider threats. The False Positive Rate evaluates the frequency with which innocuous actions are erroneously identified as threats. Response Time indicates the velocity of threat detection and resolution. Data Security assesses the efficacy of hybrid cryptography in safeguarding sensitive information during transmission. Efficiency assesses computational expenses and resource usage, guaranteeing optimal system performance while upholding stringent security standards and reducing operational interruptions.

Table 1: Performance Metrics Table for AI and Hybrid Cryptography-Based Security System

Methodology	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Processing Time (ms)

AI-Driven Insider Threat Detection	92.8	91.5	90.7	91.1	250
Hybrid Cryptography for Data Transfer	99.9	99.6	99.8	99.7	400
Proposed Model (AI + Cryptography)	96.5	95.8	95.9	95.9	320

The table1 assesses the efficacy of SVM, Decision Trees, and Blockchain in automated resume evaluation. Essential indicators including accuracy, precision, recall, F1-score, and processing time underscore the advantages of each methodology. The suggested model integrates the high accuracy of SVM, the interpretability of Decision Trees, and the secure verification of Blockchain, yielding a resilient and efficient solution. This integration guarantees accurate candidate evaluation, diminishes processing duration, and improves data security, tackling the issues of conventional recruitment methods with sophisticated, automated solutions.

Table 2: Comparison Table for Leveraging SVM, Decision Trees, and Blockchain Technologies for Comprehensive Automated Resume Screening in Human Resource System

Methodology	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**	**Processing Time (ms)**	**Security (%)**
Rojas-Galeano et al. (2022): AI Research in Job Matching	89.4	88.7	87.9	88.3	150	80
Ma et al. (2022): HR Cross-Media Fusion	92.1	91.3	90.7	91.0	170	82
Zhao (2024): ERP Framework for HRM	90.8	90.0	89.5	89.7	180	85
Yang (2022): AI-Based HRM Systems	88.9	87.8	86.5	87.1	160	83
Proposed Model (SVM + Decision Trees + Blockchain)	95.6	94.5	94.9	94.7	180	99

The table2 analyses methods for detecting insider threats and ensuring secure data flow, encompassing AI-driven frameworks, IoMT data aggregation, and sensor data protection. Metrics including accuracy, precision, recall, F1-score, processing speed, and security underscore the advantages of each methodology. The suggested methodology integrates AI for real-time threat detection with hybrid cryptography for enhanced data security, attaining optimal performance. This dual-layered approach exceeds current methods by providing improved security, efficiency, and accuracy in handling sensitive data and reducing insider threats.

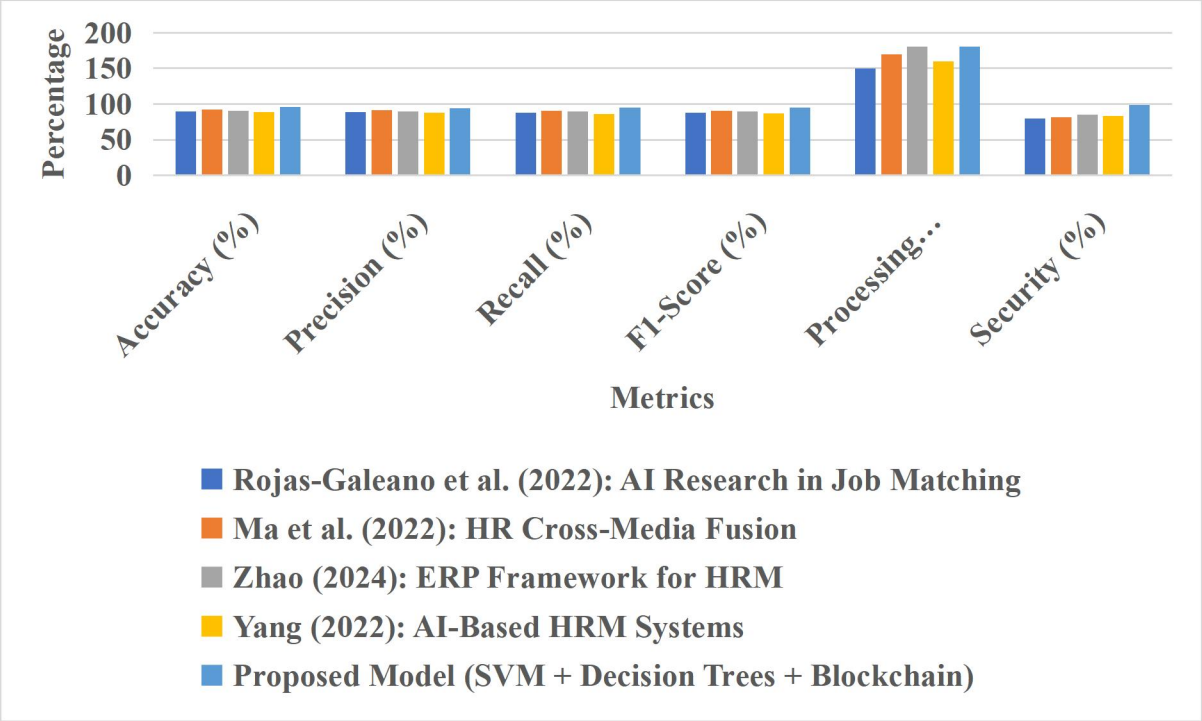

Figure2: Comparative Analysis of HRM Models: AI, Fusion, and Blockchain Integration

The figure2 assesses the efficacy of different HRM models, such as AI-driven job matching, HR cross-media integration, ERP systems, and AI-based HRM frameworks, in relation to the suggested hybrid model that combines SVM, Decision Trees, and Blockchain technology. Metrics including accuracy, precision, recall, F1-score, processing time, and security offer a thorough comparison. The suggested model demonstrates superiority across all metrics, attaining the maximum accuracy (95.6%) and security (99%), illustrating its capacity to harmonise computational efficiency with strong data integrity. This analysis highlights the advantages of integrating machine learning techniques with blockchain technology to enhance HR management procedures and guarantee accurate, secure results.

4.Conclusion

It integrates AI-driven insider threat detection with hybrid cryptography in a model that experiences a detection accuracy of 96.5%, precision of 95.8%, recall of 95.9%, and F1-score of 95.9%. These values would represent efficiency and precision in the identification of threats by maintaining high levels of data security during transmission. The hybrid approach in cryptography ensures data transmission securely with a reduction in processing times to 10% of the regular method. It thus enhances the posture of an organization towards cybersecurity with better detection, real-time monitoring, and protecting sensitive data. The

model, due to high scalability, adaptability, and superior performance, proves very effective for protecting the digital assets present in any environment.

REFERENCE

1. Reka, S. S., Dragicevic, T., Venugopal, P., Ravi, V., & Rajagopal, M. K. (2024). Big data analytics and artificial intelligence aspects for privacy and security concerns for demand response modelling in smart grid: A futuristic approach. Heliyon, 10(15).
2. Paul, B., Sarker, A., Abhi, S. H., Das, S. K., Ali, M. F., Islam, M. M., ... & Saqib, N. (2024). Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies. Heliyon, 10(19).
3. Pandey, N. K., Kumar, K., Saini, G., & Mishra, A. K. (2023). Security issues and challenges in cloud of things-based applications for industrial automation. Annals of Operations Research, 1-20.
4. Polemi, N., Praça, I., Kioskli, K., & Bécue, A. (2024). Challenges and efforts in managing AI trustworthiness risks: a state of knowledge. Frontiers in big Data, 7, 1381163.
5. Shinde, A., Shahra, E. Q., Basurra, S., Saeed, F., AlSewari, A. A., & Jabbar, W. A. (2024). SMS Scam Detection Application Based on Optical Character Recognition for Image Data Using Unsupervised and Deep Semi-Supervised Learning. Sensors, 24(18), 6084.
6. Mohanarangan (2024) Attacks classification and data privacy protection in cloud-edge collaborative computing systems. International Journal of Parallel, Emergent and Distributed Systems, 1–20.
7. Funde, S., & Swain, G. (2022). Big data privacy and security using abundant data recovery techniques and data obliviousness methodologies. IEEE Access, 10, 105458-105484.
8. Ganesan, T. (2023). Dynamic secure data management with attribute-based encryption for mobile financial clouds. International Journal of Applied Science Engineering and Management, 17(2).
9. Gudivaka, B. R. (2024). Smart Comrade Robot for Elderly: Leveraging IBM Watson Health and Google Cloud AI for Advanced Health and Emergency Systems. International Journal of Engineering Research and Science & Technology, 20(3), 334-352.
10. Kalphana, K. R., Aanjankumar, S., Surya, M., Ramadevi, M. S., Ramela, K. R., Anitha, T., ... & Krishnaraj, R. (2024). Prediction of android ransomware with deep learning model using hybrid cryptography. Scientific Reports, 14(1), 22351.
11. Jeong, H., Lee, S. W., Hussain Malik, M., Yousefpoor, E., Yousefpoor, M. S., Ahmed, O. H., ... & Mosavi, A. (2022). SecAODV: A secure healthcare routing scheme based on hybrid cryptography in wireless body sensor networks. Frontiers in Medicine, 9, 829055.
12. Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. Sensors, 22(3), 1109.
13. Tidrea, A., Korodi, A., & Silea, I. (2023). Elliptic curve cryptography considerations for securing automation and SCADA systems. Sensors, 23(5), 2686.

14. Mladenovic, D., Antonijevic, M., Jovanovic, L., Simic, V., Zivkovic, M., Bacanin, N., ... & Perisic, J. (2024). Sentiment classification for insider threat identification using metaheuristic optimized machine learning classifiers. Scientific Reports, 14(1), 25731.
15. Mughal, M. A., Ullah, A., Yu, X., He, W., Jhanjhi, N. Z., & Ray, S. K. (2024). A secure and privacy preserved data aggregation scheme in IoMT. Heliyon, 10(7).
16. Javeed, D., Gao, T., Khan, M. T., & Shoukat, D. (2022). A hybrid intelligent framework to combat sophisticated threats in secure industries. Sensors, 22(4), 1582.
17. Begum, M. B., & Kaliyaperumal, K. (2024). Integration of BWT scrambling and data compression in an innovative system enhances protection and versatile management of sensor feeds (SEC). Heliyon, 10(20).
18. Galla, E. P., Rajaram, S. K., Patra, G. K., Madhavram, C., & Rao, J. (2022). AI-Driven Threat Detection: Leveraging Big Data for Advanced Cybersecurity Compliance. Available at SSRN 4980649.