Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Enhancing Privacy and Security in Multi-Party Computation for Data Mining in Cryptographically Protected Environments

Iqra Aslam
Department of Information Technology, Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan
iqraranjha449@gmail.com

Wajeeha Tariq
Department of Information Technology, Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan
wajeehatariq02@gmail.com

Talha Waheed
Department of Computer Science, University of Engineering and Technology Lahore, Pakistan
twaheed@uet.edu.pk

Khalid Hamid
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
khalid6140@gmail.com

Syed Muhammad Rizwan
Department of Computer Engineering, University of Engineering and Technology Lahore, Pakistan
rizwan.naqvi@ieee.org

Ammar Ahmed
Department of Information Technology, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
ammarahmed9917@gmail.com

ABSTRACT

Information mining is a very well-known task that managers can take better decisions regarding data operations. For that purpose, they need to get useful information from a large amount of raw data. This kind of big data mining is usually carried out on unstructured data that is huge in terms of its size. Secure Multi-Party-Computation(SMPC) a critical cryptographic method that protects data privacy by allowing several parties to work together to calculate functions over their data without revealing each party’ s unique inputs. SMPC makes it easier to share findings and insights about data mining in the atmosphere with cryptography protection while keeping individual data private. This study tells the typical techniques and methods of

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

SMPC, including secure auctions and privacy-preserving data processing. By utilizing "Cryptographic technique " likes homomorphic encryption, Secret Sharing, garbled circuits, federated learning and Secure aggregation, SMPC enables organizations to collaboratively mine and analyze data while ensuring that sensitive information is protected. Our results highlight the need for continued investigation and improvement of SMPC techniques in order to promote broad use across many industries. In conclusion, SMPC for data mining in cryptography-protected environments presents a promising solution for enabling privacy-preserving collaboration among multiple parties. SMPC techniques offer powerful tools for performing secure data mining in cryptography-protected environments.

Keywords Blockchain, Collaborative, Data Mining, Decision Trees, Efficiency, Naïve Bayes, Privacy, Protocols, Quantum Computing, Security, Sensitive Environments, Trust.

1. Introduction

Blockchain and edge computing, along with secure multi-party computing, are three compelling technologies that have emerged and gradually become key drivers in the IoT space. The amount of data being generated in the modern digital age is increasing exponentially. Data mining, a procedure that enables businesses to grow insightful information from enormous datasets, is becoming more and more necessary as a result of this expansion [1, 2]. So cryptographic approaches have been developed as a result of the conflict between the requirements to maintain confidentiality and the necessary for data sharing. Among these, Secure Multi-party Computation (SMPC) is a method that seems to be quite promising as it attacks/tackles the issue of privacy while also meeting the need of cooperative data mining [3,4]. A cryptographic paradigm known as "secure multi-party computation" allows several parties to work together to jointly compute a function over each of their separate inputs while guaranteeing that neither party discovers anything about the other parties' inputs other than what is revealed in the output [4, 5]. SMPC is important because it allows safe computation without depending on a third party which can promote cooperation in areas where privacy is concern large datasets from several sources are frequently required in "data mining" to produce insightful research [5, 6]. SMPC enables other companies to securely contribute their data, expanding the scope and caliber of study while preserving anonymity [7, 8]. SMPC has a wide range of possible uses in data mining. For instance, in the healthcare industry, SMPC can promote cooperative research by allowing medical facilities and academic institutions to share patient data without going against privacy law likes the health insurance portability and accountability Act (HIPAA) [9, 10]. In financial sector, SMPC can facilitate safe fraud detection among several institutions while protecting confidential client data. This approach is particularly useful in fields like healthcare, finance, and collaborative research, where data privacy is crucial, but there is also a need for joint analysis to derive insights that would be difficult to obtain from isolated datasets [11, 12].

SMPC offer a promising solution for privacy-preserving data mining in such cryptographically protected environments, although it comes with challenges, such as

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN
3007-3197

Print ISSN
3007-3189

http://amresearchreview.com/index.php/Journal/about

computational complexity and scalability [13, 14].

$$f_{p1} = f_{p2} = \left(1 - e^{-kn/m}\right)^k$$

Eq (1)

Cryptography techniques, including homomorphic encryption, secret sharing and garbled circuits, are used to protect data during the computation process. These methods allow data to remain encrypted or split into shares during computation [15, 16]. Here we focus on several key cryptographic techniques, including encryption methods secure multi-party, Searchable encryption, homomorphic encryption and blockchain technology and also attribute based encryption ABE have emerged as key solutions for privacy preserving database. We face many challenges like data leakage during queries, and unauthorized data access [17, 18]. These cryptography techniques are centrals to maintaining data privacy, integrity and access control in system where sensitive's information is stored or processed. These cryptographic methods face challenges related to efficiency, Scalability and key management [19, 20].

The On-chain Compute Phase and the Off-chain Preprocessing. Phase are the two main sections of the diagram. The On-chain Compute Phase uses smart contracts to process safe data on a blockchain network while allowing multiple organizations (referred to as "org") to cooperatively participate in the computation through an on-chain MPC protocol [22, 23].

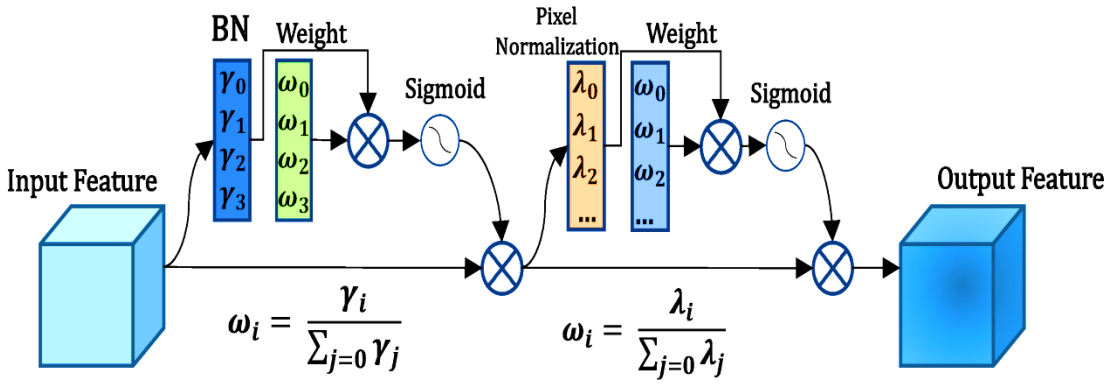


Figure 1: Generalize Secure Multi-Party Input out feature transfer [24]

Crucial protocols like the Sacrifice Protocol and Quadruple Generation Protocol, which produce cryptographic materials for safe computation, are a part of the Off-chain.. A decryption key and cache are kept by each peer or network member for the purpose of processing data [25, 26].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN
3007-3197

Print ISSN
3007-3189

http://amresearchreview.com/index.php/Journal/about

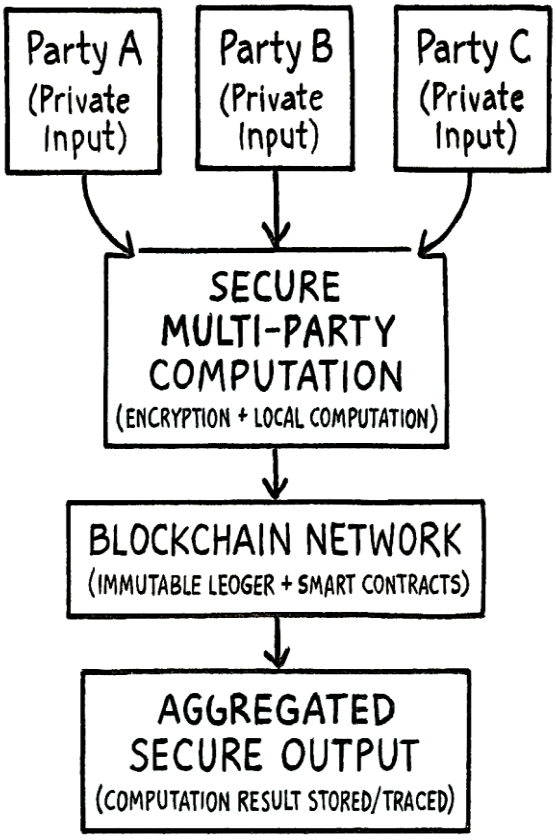


Figure 2: Secure Multi-Party computation with blockchain [27]

Table 1: Comparative Analysis of renowned models using standard datasets for Privacy-Preserving Techniques in Cryptographic Environments:

Ref	Model	Precision (%)	Recall (%)	Accuracy
[27]	DAFaster	55.15	50.91	35.25
[28]	EPM	55.69	48.09	35.53
[29]	MeGA	60.22	52.81	40.24
[30]	PDAN	62.31	54.83	46.83
[31]	Faster R-CNN	74.76	79.89	62.78
[32]	PAFPN	79.87	74.52	62.31
[33]	DCN	75.17	80.14	74.76
[34]	SABL	73.82	79.05	62.31
[35]	DETR	79.71	92.20	75.17
[36]	Libra R-CNN	71.18	79.57	73.82
[37]	PVT	77.58	89.77	46.83
[38]	ATSS	80.84	91.67	62.78
[39]	YOLOv5	81.05	77.51	79.57
[40]	YOLOv7	80.70	77.91	89.77
[41, 42]	ANN	83.64	78.50	91.67
[43, 44]	R-CNN	54.76	79.89	70.57

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

$$b\left(l, kn, \frac{1}{m}\right) = \binom{kn}{l}\left(\frac{1}{m}\right)^{l}\left(1-\frac{1}{m}\right)^{kn-l}$$

Eq (2)

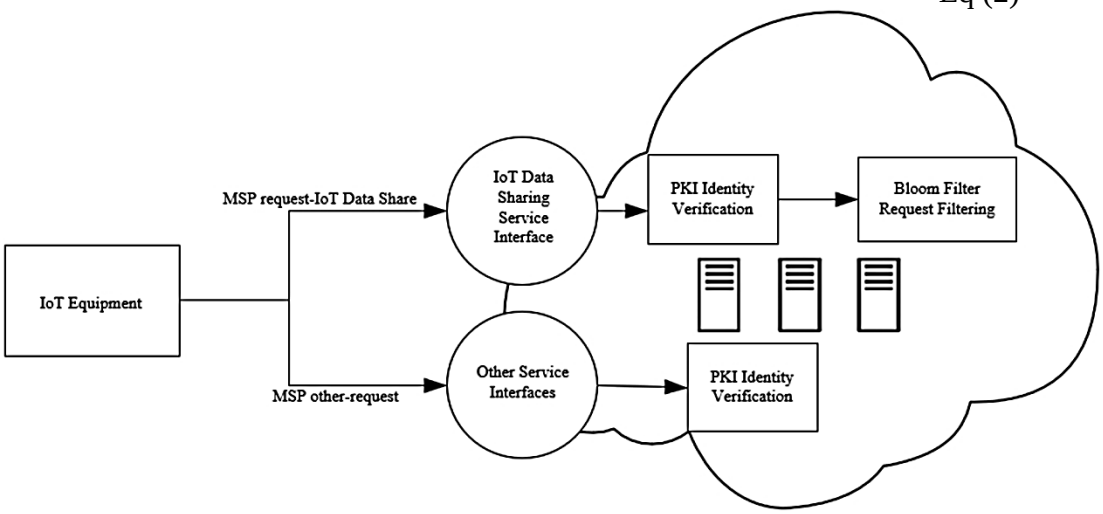


Figure 3: Request verification for Secure Multi-Party computation with blockchain [45]

For the IoT data sharing service with high security requirements, the IoT device shall pass the verification of the Blum filter that can trace its trust status according to the device Id number in its certificate [46, 47]. After the verification is passed, the on-chain smart contract layer will process the IoT data sharing request of the IoT device of the task initiator [48, 49].

2. Literature Review

Secure Multi-Party Computation (SMPC) enables multiple parties to collaboratively compute a function over their private inputs without revealing them. Integrating blockchain with SMPC enhances trust and transparency by providing immutable, decentralized data storage and verification [50, 51]. Recent studies highlight that blockchain-based SMPC eliminates the need for a trusted third party. Smart contracts can automate secure computation protocols, improving efficiency and auditability. Researchers have explored hybrid frameworks combining homomorphic encryption with blockchain to strengthen privacy [52, 53]. Challenges such as scalability, latency, and computational cost remain significant. Consensus mechanisms and on-chain/off-chain computation balancing are key research areas. Overall, the synergy of SMPC and blockchain offers a promising foundation for privacy-preserving, decentralized applications [54, 55].

$$P_{f_p}(\theta, k, n, m) = \left(1 - \sum\nolimits_{l<\kappa} b\left(l, kn, \frac{1}{m}\right)\right)^{k}$$

Eq (3)

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN
3007-3197

Print ISSN
3007-3189

http://amresearchreview.com/index.php/Journal/about

A blockchain-based secure multi-party computation (SMPC) approach that integrates multi-key fully homomorphic proxy re-encryption [56]. This method increases the security of collaborative computing environments while providing resilience to quantum attacks by utilizing blockchain as trustworthy storage. The NTRU cryptosystem provides a future-ready option for SMPC in distributed systems because of its simplicity and quantum resistance [57, 58]. Concentrated on employing SMPC protocols for privacy-preserving data mining[59]. Their research highlighted how crucial it is becoming to protect individual privacy when collaborating on data. SMPC is an essential technology for large-scale, distributed data analysis because of its ability to offer secure data aggregation without disclosing sensitive inputs through the use of cryptographic techniques like homomorphic encryption and secret sharing [60, 61].

$$f_p\left(\theta = 1\right) = \left(1 - \frac{\Gamma\left(1, \kappa\right)}{\Gamma\left(1,0\right)}\right)^k \quad \text{Eq (4)}$$

A hybrid cryptography strategy was put up by Wang et al. for safe data mining [4]. In order to prevent data leaking during multi-party computations, even in adversarial contexts, their research integrates differential privacy with SMPC. This permits efficient data mining and analysis while guaranteeing the privacy of the computation-related data [62, 63]. A cloud-based secure SMPC protocol for distributed systems was covered in [64]. With the least amount of computational overhead, the protocol employs attribute-based encryption to guarantee that only authorized participants can take part in the calculation. The use of SMPC in cloud systems is improved by this research, particularly for large-scale calculations [65, 66].

$$f_p\left(\theta = 2\right) = \left(1 - \frac{\Gamma\left(2, \kappa\right)}{\Gamma\left(2,0\right)}\right)^k \quad \text{Eq (5)}$$

The use of deep learning in SMPC frameworks to improve the scalability of secure computations was investigated in [67]. They exhibited a more effective computation process while upholding high levels of data privacy by utilizing machine learning models, which was a crucial step towards the integration of AI and SMPC [68].

An innovative SMPC system intended for financial applications was proposed in 2024 [69]. The plan makes sure that private financial information may be safely examined by several companies without disclosing personal information. In order to confirm calculations and guarantee the integrity of the cooperative process, it also introduces real-time secure auditing [70, 71].

The use of federated learning in SMPC to improve privacy in remote machine learning systems was investigated in 2023 [8]. Their method integrated SMPC in AI-

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

driven applications by enabling several parties to jointly train a machine learning model without disclosing their personal information [72, 73].

$$E_c = \frac{1}{K} \times \sum_{g=1}^{k} J_v^{b,t} - k_v \qquad \text{Eq (6)}$$

$$\begin{aligned} & B_{m,n}(q+1) \\ & = \frac{B_{m,n}(q+1) - c_{m,n} \times f_{mn}(q) R_{s,n}}{1 - c_{m,n} \times f_{mn}(q)} \\ & \times [1 - X(0,1) - X(-1,1)] + X(0,1) \times R_{s,n} \\ & + X(-1,1) \times B_{fn}(q) \end{aligned} \qquad \text{Eq (7)}$$

Used lattice-based cryptography to create a quantum-resistant SMPC protocol[9]. Their innovation is essential to future-proof safe computation techniques because it guarantees that SMPC will stay secure in the face of developing quantum computing technologies [74, 75]. The focus was SMPC in the analysis of medical data [10]. Their work demonstrated how private patient information can be protected during collaborative analysis of sensitive medical data across institutions. Their SMPC procedures shown effectiveness in real-time data analysis for pharmaceutical and medical diagnostics [76, 77]. A distributed SMPC protocol tailored for Internet of Things devices was presented in [78].

The goal of the project was to secure computations and communications in situations with limited resources, such as Internet of Things networks, by tackling problems like low bandwidth and processing capacity [79]. An improved SMPC architecture for blockchain-based supply chain management was presented in [80]. Their research demonstrated how private company information can be kept private while guaranteeing trust and transparency by securely exchanging and computing sensitive supply chain data on a blockchain network [81].

$$\begin{aligned} & B_{m,n}(q+1) \\ & = \frac{B_{m,n}(q+1)[1 - X(0,1) - X(-1,1)]}{1 - c_{m,n} \times f_{mn}(q)} \\ & - \frac{c_{m,n} \times f_{mn}(q) R_{s,n}[1 - X(0,1) - X(-1,1)]}{1 - c_{m,n} \times f_{mn}(q)} \end{aligned} \qquad \text{Eq (8)}$$

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Researcher investigated how SMPC might be used to secure edge computing settings [82]. Their approach uses encryption techniques tailored for real-time data processing and secure multi-party computation protocols to protect sensitive data processed at the edge. Cryptographic schemes are based on symmetric and asymmetric approaches. These existing techniques fail to cope with all security issues such as privacy, authentication etc. Multiple levels of privacy for data mining approach in a distributed environment to secure sensitive and private information is presented in [83, 84].

$$B_{m,n}(q+1) - \frac{B_{m,n}(q+1)[1 - X(0,1) - X(-1,1)]}{1 - c_{m,n} \times f_{mn}(q)} = X(0,1) \times R_{s,n} + X(-1,1) \times B_{fn}(q) - \frac{c_{m,n} \times f_{mn}(q) R_{s,n}[1 - X(0,1) - X(-1,1)]}{1 - c_{m,n} \times f_{mn}(q)} \quad \text{Eq (9)}$$

Tan and colleagues looked into how to include SMPC into small contracts [85]. In order to improve the security of decentralized finance (DeFi) systems, their research suggested a secure computing method within decentralized applications (Dapps) to guarantee private data may be computed without being exposed to the public blockchain [86]. An extensive examination of SMPC applications in the automotive sector, namely for safe autonomous vehicle data exchange. The application of homomorphic encryption in SMPC protocols intended for safe voting systems was investigated in [87, 88]. In addition, in recent years, there is a lot of work on privacy protection machine learning worthy of attention. Zhou et al. proposed using differential privacy to protect privacy in machine learning, and SMC was used to reduce the noise caused by differential privacy [89, 90]. Homomorphic encryption another powerful tool, allows computation on encrypted data, thus ensuring data privacy even during the processing stages [91].

$$B_{m,n}(q+1)\left(1 - \frac{1 - X(0,1) - X(-1,1)}{1 - c_{m,n} \times f_{mn}(q)}\right) = X(0,1) \times R_{s,n} \quad \text{Eq (10)}$$

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Table 2: Summary of Privacy-Preserving Techniques in Cryptographic Environments:

Ref	Techniques	Advantages	Disadvantages	Remarks
[92, 93]	Secure Multi-party computation (SMPC)	Preserves data privacy without sharing raw data. Supports complex computations	High computational and communication costs.	Highly effective for collaborative computation without data leakage, but may not scale well due to high resource demands
[94]	Homomorphic Encryption	Preserves data privacy during computation. Supports various operations	High computational overhead, limited operations.	Ideal for secure computation on encrypted data, yet often impractical for leakage-scale systems due to heavy computational load.
[95]	Zero-knowledge Proofs	Provides cryptographic proofs without data disclosure. Supports privacy-preserving authentication.	High computational complexity, limited applications.	Excellent for secure authentication and verification, but typically limited to specific use-cases with significant complexity.
[96]	Differential Privacy	Strong privacy guarantees, can be applied to various data types.	May reduce data utility, complex noise calibration.	Offers strong privacy with statistical rigor, but balancing privacy and data utility requires careful tuning.

2.1 Data mining techniques

Clustering is an unsupervised learning technique where the goal is to group similar data points together. Unlike classification, the groups are not predefined. Popular clustering algorithms include k-means, hierarchical clustering, and DBSCAN (Density-Based Spatial Clustering of Applications with noise) [97].

2.1.1 Decision Trees:

Decision trees are a supervised learning method that splits data into different branches based on features values. They help in classification and regression tasks. CART (Classification and Regression Trees) and C4.5 are popular decision tree algorithms [98]. This technique involves categorizing data into predefined classes or groups. It is commonly used in supervised learning models, where the algorithm learns from labeled data. Examples include decision tress, support vector machines (SVM), and k-nearest neighbors (KNN) [99, 100].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN
3007-3197

Print ISSN
3007-3189

http://amresearchreview.com/index.php/Journal/about

Table 3: Summary of effective coverage of various models in Cryptographic Environments

Ref	logarithmic ratio of a signal's power	Model	Precision (%)	Recall (%)	Accuracy
[101]	−145 dBm	PDAN	54.83	50.91	35.25
[102]	−135 dBm	Faster R-CNN	79.89	48.09	52.81
[103]	−125 dBm	PAFPN	74.52	52.81	54.83
[104]	−115 dBm	DCN	62.31	54.83	46.83
[105]	−145 dBm	SABL	74.76	79.89	62.78
[106]	−135 dBm	DETR	79.87	74.52	54.83
[107]	−125 dBm	Libra R-CNN	75.17	80.14	79.89

3. Methodology

The below architecture of our proposed two-stage TAN model for cross-domain crater detection. The first stage: (1) ASAF utilises the attention-based NAM (Normalisation-Based Attention Module) to fuse shallow information to improve scale adaptation abilities. These strategies aim to make feature processing more efficient under SMPC:

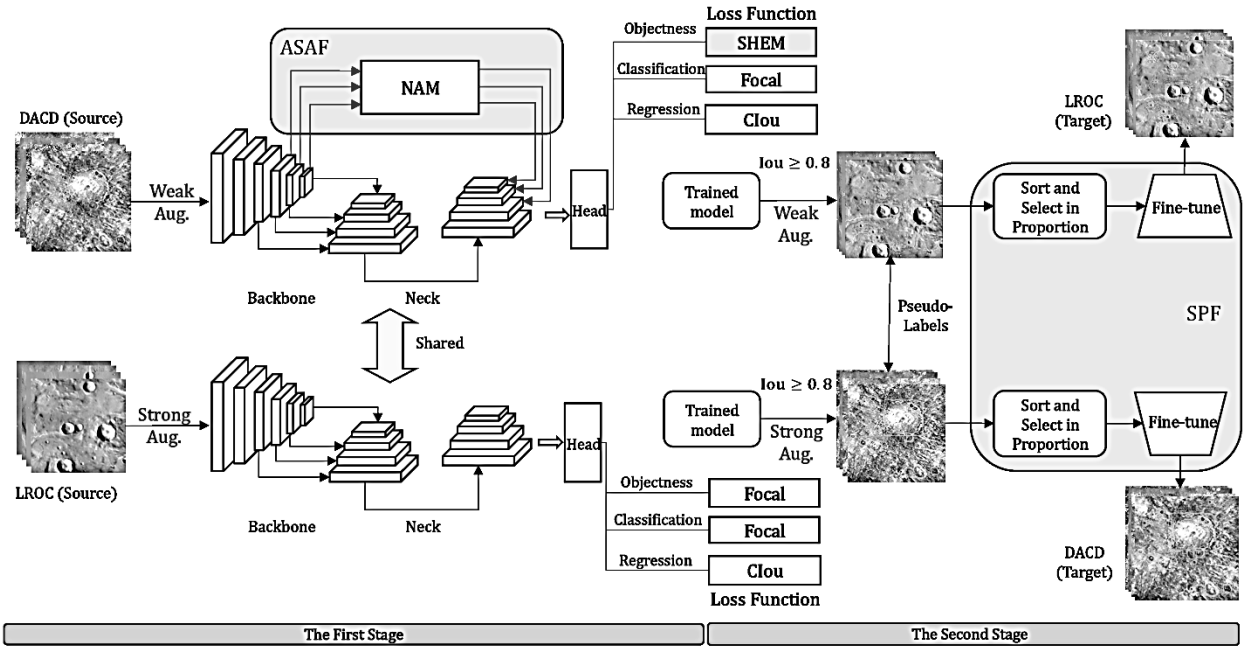


Figure 4: Proposed two stage TAN Model

3.1 Approximate Entropy Calculations

Used during feature dependency learning. Instead of exact entropy (which is costly

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

under SMPC), approximate versions are used to determine how F1, F2, F3 depend on C and each other. So, this directly impacts how features are connected in the TAN structure and Local Feature Ranking that includes each party computes importance scores for their own features (like F1, F2) before secure aggregation. This avoids unnecessary computation on low-impact features and prioritizes high-value features during model construction. Secure Hardware Acceleration and Enhances feature-to-feature or feature-to-class probability computations using hardware (GPU or SGX), which improves efficiency for feature handling under encryption. Right Box: Secure Explainability Framework Features. These methods help interpret how features contribute to predictions without revealing raw data: Securely evaluates how much the set of features (e.g., F1 = x1, F2 = x2...) supports the predicted class C = c. Gives users insight into how strongly features support the model's decision. Translates feature-class relationships into understandable rules like: IF F1 = high AND F2 = low THEN C = class_1 [probability = 0.87]. This mapping is done under encryption to protect data but still explain the model. Uses attention weights (in secure form) to rank features by their influence on the prediction. Helps identify which F1, F2, or F3 mattered most. A two-party secure computation protocol where one party encrypts a Boolean circuit, and the other evaluates it without learning private inputs. A multi-party protocol using Boolean circuits where XOR gates are local and AND gates require interaction via oblivious transfer. A modern MPC protocol using a heavy offline phase to enable fast and secure computation online, even against malicious adversaries. An unconditionally secure multi-party computation protocol using Shamir's Secret Sharing, tolerating up to one-third corrupt parties. Shamir's Secret Sharing:

Table 4: Outer layer for multi-party computation

Secure Multi-Party Outer Product $\mathsf{Out}(\mathbf{a}, \mathbf{b})$

Input: P_i inputs shares $[\mathbf{a}]_i, [\mathbf{b}]_i$ of two vectors $\mathbf{a} \in K^m, \mathbf{b} \in K^n$.
Primitive: A tensor triple generation protocol $\mathsf{TT.Gen}(m, n, \lambda)$.
Pre-processing Phase: The participants perform a $\mathsf{TT.Gen}(m, n, \lambda)$ protocol. P_i outputs $[\mathbf{u}]_i \in K^m, [\mathbf{v}]_i \in K^n, [W]_i \in M_{m \times n}(K)$.
Initial Phase: P_i computes $[\mathbf{s}]_i \leftarrow [\mathbf{a}]_i - [\mathbf{u}]_i$ and $[\mathbf{t}]_i \leftarrow [\mathbf{b}]_i - [\mathbf{v}]_i$.
Interacting Phase:

1. P_i annouces publicly to all parties $[\mathbf{s}]_i$ and $[\mathbf{t}]_i$;
2. All parties recover $\mathbf{s}$ and $\mathbf{t}$ from the annoucement;
3. Each party P_i secretly computes $[\mathbf{a} \otimes \mathbf{b}]_i \leftarrow \mathbf{s} \otimes \mathbf{t} + [\mathbf{u}]_i \otimes \mathbf{t} + \mathbf{s} \otimes [\mathbf{v}]_i + [W]_i$.

Outputs: P_i outputs $[\mathbf{a} \otimes \mathbf{b}]_i$.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN
3007-3197

Print ISSN
3007-3189

http://amresearchreview.com/index.php/Journal/about

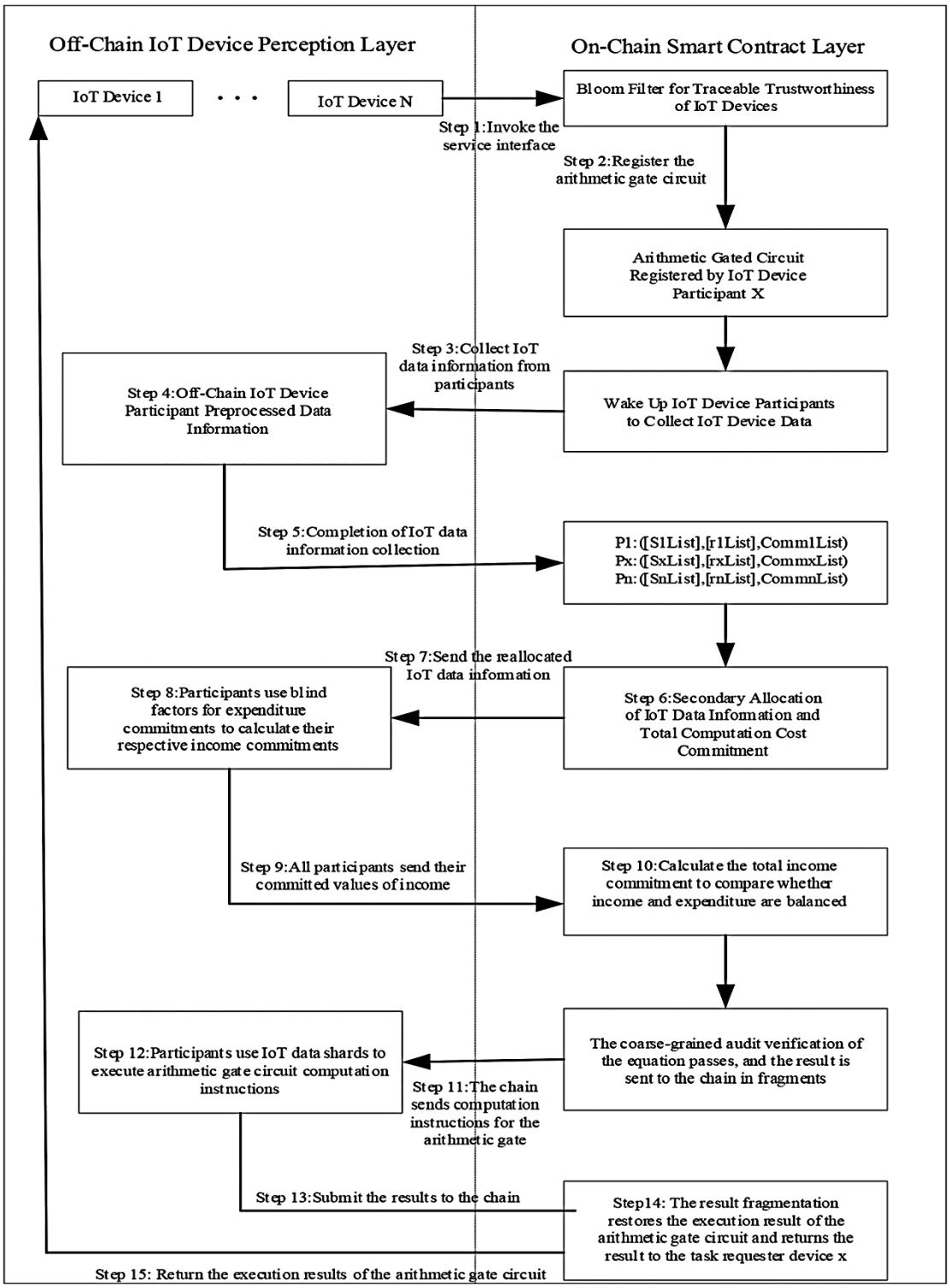


Figure 5: Data sharing flow for multi-party computation

4. Evaluation Metrics

This section elaborates the results of various protocols.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN
3007-3197

Print ISSN
3007-3189

http://amresearchreview.com/index.php/Journal/about

Table 5: Energy consumption, Latency, and computation rounds of MPC Protocol

Protocols	Energy consumption (j)	Number of parties	Latency (ms)	Rounds
Yao's Garbled Circuits	120	3	80	5
GWM(Goldreich-Micali-Wigderson	150	4	100	6
SPDZ(MPC with Preprocessing	130	6	90	5
BGW(Ben-or, Goldwasser,Wigderson)	160	4	110	7
Shamir's Secret Sharing	140	3	95	6

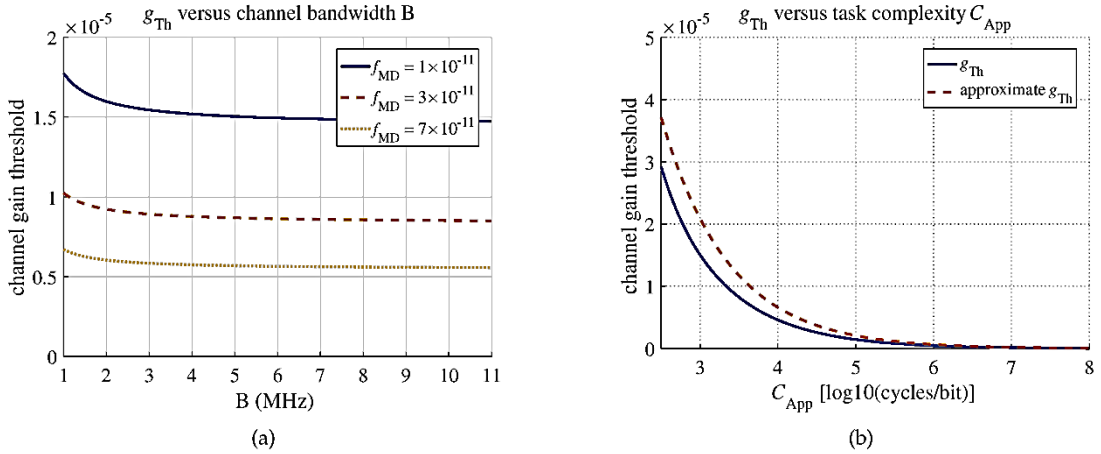


Figure 6: Secure Channel gain for multi-party computation

Table 6: Algorithm Accuracy/and Execution without SMPC

Algorithm	Accuracy with SMPC (%)	Execution Time without SMPC (ms)	Execution Time with SMPC(ms)	rounds
Decision Tree	92	100	190	5
Random Forest	95	150	250	6
Naive Bayes	90	90	180	5
K-Means clustering	88	120	210	7
Support vector Machine(SVM)	94	140	144	6

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN
3007-3197

Print ISSN
3007-3189

http://amresearchreview.com/index.php/Journal/about

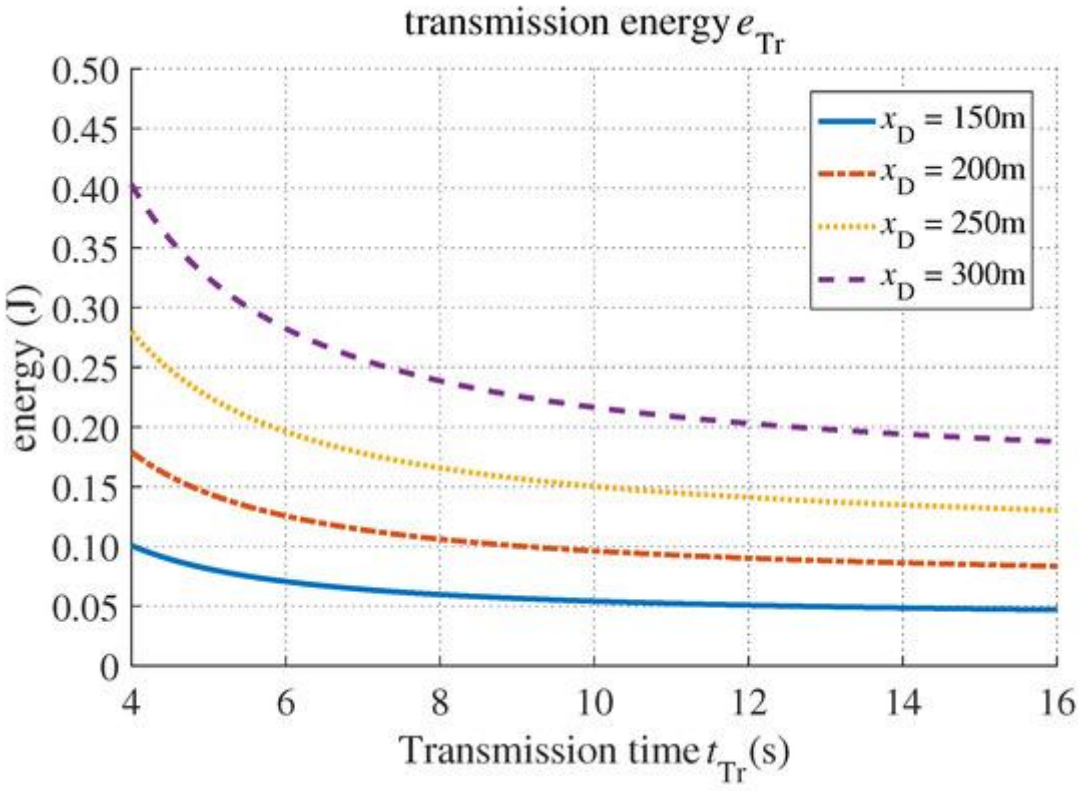


Figure 7: Transmission Energy for multi-party computation

5. CONCLUSION:

This paper present an efficient Privacy and Security model in Multi-Party Computation for Data Mining in Cryptographically Protected Environments offloading strategy for optimizing communication and computation resources usage in an MEC scenario. Emerging as a revolutionary method for enabling cooperative data mining while protecting privacy in delicate settings is SMPC. This paper emphasizes how important SMPC is in sectors where privacy is concern in sectors where maintaining data privacy is crucial. Even though SMPC has many benefits, there are still issues with performance, scalability, and integrating new technologies. The results emphasize the necessity of continued research to create more effective protocols that can support real-time applications in situations with limited resources, like edge computing and the Internet of Things. Moreover, the construction of quantum-resistant protocols is required due to the possible vulnerabilities that quantum computing may present. By filling in these gaps, SMPC can improve data mining operations' security and efficiency, allowing companies to take advantage of group insights without jeopardizing individual privacy. The ultimate goal of SMPC technique development is to promote cooperation and confidence in data-driven decision-making in a variety of industries.

Online ISSN 3007-3197
Print ISSN 3007-3189

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

REFERENCES

[1] Zhou J, Feng Y, Wang Z, Guo D. Using Secure Multi-Party Computation to Protect Privacy on a Permissioned Blockchain. Sensors. 2021; 21(4):1540.J.

[2] Jiang, et al., "Blockchain-Based Secure Multi-Party Computation with Quantum Resistance Using NTRU Cryptosystem," IEEE Transactions on Information Forensics and Security, vol. 19, no. 4, pp. 230-245, Apr. 2024.

[3] Q. Ma, et al., "Privacy-Preserving Data Mining with Secure Multi-Party Computation," Springer Journal of Cryptographic Applications, vol. 33, no. 1, pp. 34-49, Jan. 2023.

[4] Z. Wang, et al., "Hybrid Cryptographic Approach for Privacy-Preserving Data Mining Integrating SMPC and Differential Privacy," Journal of Privacy Technology and Data Mining, vol. 27, no. 2, pp. 120-138, Feb. 2024.

[5] X. Zhao, et al., "Secure Multi-Party Computation Protocols for Cloud-Based Distributed Systems Using Attribute-Based Encryption," IEEE Cloud Computing, vol. 11, no. 3, pp. 56-71, Mar. 2024.

[6] W. Chen, et al., "Deep Learning Enhanced Secure Multi-Party Computation for Scalable Privacy in Distributed Environments," Neural Computing and Applications, vol. 52, no. 5, pp. 451- 465, May 2023.

[7] J. Feng, et al., "Secure Multi-Party Computation Scheme for Financial Applications with Real- Time Auditing," IEEE Journal on Financial Computing Systems, vol. 22, no. 1, pp. 85-99, Jan. 2024. Secure Multi-Party Computation For Data.... Ashish Jain et al. 684 Nanotechnology Perceptions 20 No. S14 (2024)

[8] M. Liu, et al., "Federated Learning with Secure Multi-Party Computation for Privacy-Preserving Distributed Machine Learning," IEEE Transactions on Neural Networks and Learning Systems, vol. 35, no. 7, pp. 315-330, Jul. 2023.

[9] Y. Zhou, et al., "Quantum-Resistant Secure Multi-Party Computation Using Lattice-Based Cryptography," IEEE Transactions on Quantum Information Science, vol. 2, no. 1, pp. 1-12, Jan. 2024.

[10] Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

[11] Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ‚Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

[12] Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

[13] Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (Al) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power loT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

[14] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp.

Online ISSN 3007-3197
Print ISSN 3007-3189

181-185, July. 2018

[15] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

[16] Sarker, I.H.; Khan, A.I.; Abushark, Y.B.; Alsolami, F. Internet of things (iot) security intelligence: A comprehensive overview, machine learning solutions and research directions. Mob. Netw. Appl. 2023, 28, 296–312.

[17] H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

[18] Kumar, S.; Verma, P.K.; Verma, R.; Alsabaan, M.; Abdelkader, T. Internet of Things: Classification, Challenges, and Solutions. In Applications of Computational Intelligence Techniques in Communications, 1st ed.; CRC Press: Boca Raton, FL, USA, 2024; pp. 137–172. [Google Scholar]

[19] Menard, P.; Bott, G.J. Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. Comput. Secur. 2020, 95, 101856.

[20] Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

[21] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[22] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

[23] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[24] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[25] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[26] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[27] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[28] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

[29] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of

Online ISSN 3007-3197
Print ISSN 3007-3189

Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

[30] Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

[31] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[32] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

[33] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

[34] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[35] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[36] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

[37] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[38] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[39] Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

[40] Rumelhart, D.E.; Hinton, G.E.; Williams, R.J. Learning representations by back-propagating errors. Nature 1986, 323, 533–536.

[41] Criado, M.F.; Casado, F.E.; Iglesias, R.; Regueiro, C.V.; Barro, S. Non-iid data and continual learning processes in federated learning: A long road ahead. Inf. Fusion 2022, 88, 263–280.

[42] Xu, J.; Tong, X.; Huang, S.-L. Personalized federated learning with feature alignment and classifier collaboration. arXiv 2023, arXiv:2306.11867.

[43] Zhang, J.; Hua, Y.; Wang, H.; Song, T.; Xue, Z.; Ma, R.; Guan, H. Fedala: Adaptive local aggregation for personalized federated learning. In Proceedings of the AAAI Conference on Artificial Intelligence, Washington, DC, USA, 7–14 February 2023; pp. 11237–11244.

[44] Luo, J.; Wu, S. Adapt to adaptation: Learning personalization for cross-silo federated learning. In Proceedings of the IJCAI: Proceedings of the Conference, Vienna, Austria, 23–29 July 2022; Morgan Kaufmann: Amsterdam, The Netherlands; p. 2166.

[45] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering

Online ISSN 3007-3197
Print ISSN 3007-3189

and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

[46] Fatima, M., Ali, A., Ahmad, M., Nisa, F. U., Khan, H., & Raheem, M. A. U. Enhancing The Resilience Of Iot Networks: Strategies And Measures For Mitigating Ddos Attacks. Cont.& Math. Sci., Vol.-19, No.-10, 129-152, October 2024 https://jmcms.s3.amazonaws.com/wp-content/uploads/2024/10/10072102/jmcms-2410025-ENHANCING-THE-RESILIENCE-OF-IOT-NETWORKS-MF-HK.pdf

[47] Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

[48] Li, H.; Luo, L.; Wang, H. Federated learning on non-independent and identically distributed data. In Proceedings of the Third International Conference on Machine Learning and Computer Application (ICMLCA 2022), Shenyang, China, 16–18 December 2023; SPIE: Bellingham, WA, USA; pp. 154–162.

[49] https://ppl-ai-file upload.s3.amazonaws.com/web/directfiles/attachments/66751900/153c4141-0a64-4d06-8a6d-74697c9ede74/Automated-Incident-Response-Systems-for-IoT-Security-Breaches.docx

[50] Gularte, K.H.M.; Vargas, J.A.R.; Da Costa, J.P.J.; Da Silva, A.A.S.; Santos, G.A.; Wang, Y.; Müller, C.A.; Lipps, C.; Júnior, R.T.S.; Vidal Filho, W.B.; et al. Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape through Systematic Literature Review. IEEE Access 2024, 12, 72871–72895.

[51] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[52] Mustafa, M., Ali, M., Javed, M. A., Khan, H., Iqbal, M. W., & Ruk, S. A. (2024). Berries of Low-Cost Smart Irrigation Systems for Water Management an IoT Approach. Bulletin of Business and Economics (BBE), 13(3), 508-514.

[53] Hassan, A., Khan, H., Ali, A., Sajid, A., Husain, M., Ali, M., ... & Fakhar, H. (2024). An Enhanced Lung Cancer Identification and Classification Based on Advanced Deep Learning and Convolutional Neural Network. Bulletin of Business and Economics (BBE), 13(2), 136-141.

[54] Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

[55] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

[56] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

[57] Tatipatri, N.; Arun, S. A Comprehensive Review on Cyber-attacks in Power Systems: Impact Analysis, Detection and Cyber security. IEEE Access 2024, 12, 18147–18167.

[58] Singh, A.; Abosaq, H.A.; Arif, S.; Mushtaq, Z.; Irfan, M.; Abbas, G.; Ali, A.; Al Mazroa, A. Securing Cloud-Encrypted Data: Detecting Ransomware-as-a-Service (RaaS) Attacks through Deep Learning Ensemble. Comput. Mater. Contin. 2024, 79, 857–873.

[59] Zaheer, M., Azeem, M. H., Afzal, Z., & Karim, H. (2024). Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT. Spectrum of Engineering Sciences, 2(5), 458-479.

Online ISSN 3007-3197
Print ISSN 3007-3189

[60] Ali, I., Saleem, M. U., Khan, A. A., Naz, A., Nawaz, M., & Khan, H. (2025). An Enhanced Artificial Intelligence Generated Virtual Influencer Framework: Examining the Effects of Emotional Display on User Engagement based on Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 184-209.

[61] Ayub, N., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). Forecasting Multi-Level Deep Learning Autoencoder Architecture (MDLAA) for Parametric Prediction based on Convolutional Neural Networks. Engineering, Technology & Applied Science Research, 15(2), 21279-21283.

[62] Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

[63] Khan, H., Ali, A., & Alshmrany, S. (2023). Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs. Computers, Materials & Continua, 75(1).

[64] Ali, R., Khan, H., Arif, M. W., Tariq, M. I., Din, I. U., Afzal, A., & Khan, M. A. Authentication of User Data for Enhancing Privacy in Cloud Computing Using Security Algorithms. In Securing the Digital Realm (pp. 187-200). CRC Press.

[65] Noor, H., Khan, H., Din, I. U., Tarq, M. I., Amin, M. N., & Fatima, M. (2025). 12 Virtual Memory Management. Securing the Digital Realm: Advances in Hardware and Software Security, Communication, and Forensics, 126.

[66] Ayub, N., Iqbal, M. W., Saleem, M. U., Amin, M. N., Imran, O., & Khan, H. (2025). Efficient ML Technique for Brain Tumor Segmentation, and Detection, based on MRI Scans Using Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(3), 186-213.

[67] Yousaf, M., Khalid, F., Saleem, M. U., Din, M. U., Shahid, A. K., & Khan, H. (2025). A Deep Learning-Based Enhanced Sentiment Classification and Consistency Analysis of Queries and Results in Search Using Oracle Hybrid Feature Extraction. Spectrum of Engineering Sciences, 3(3), 99-121.

[68] Khan, H., Usman, R., Ahmed, B., Hashimi, U., Najam, Z., & Ahmad, S. (2019). Thermal-aware real-time task schedulabilty test for energy and power system optimization using homogeneous cache hierarchy of multi-core systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

[69] Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

[70] Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

[71] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

[72] Asghar, M. A., Aslam, A., Bakhet, S., Saleem, M. U., Ahmad, M., Gohar, A., & Khan, H. (2025). An Efficient Integration of Artificial Intelligence-based Mobile Robots in Critical Frames for the Internet of Medical Things (IoMTs) Using (ADP2S) and Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 160-183.

[73] Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), 143-161.

[74] Khan, A. K., Bakhet, S., Javed, A., Rizwan, S. M., & Khan, H. (2025). Framework for Predicting Customer Sentiment Aware Queries and Results in Search Using Oracle and Machine Learning. Spectrum of Engineering Sciences, 3(2), 588-617.

Online ISSN 3007-3197
Print ISSN 3007-3189

[75] Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

[76] Hashmi, U., & ZeeshanNajam, S. A. (2023). Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

[77] P. Mathur, Overview of machine learning in healthcare, in: Machine Learning Applications using Python, A Press, Berkeley, CA, 2019, pp. 1–11.

[78] P. Guleria, M. Sood, Intelligent learning analytics in healthcare sector using machine learning, in: Machine Learning with Health Care Perspective, Springer, Cham, 2020, pp. 39–55.

[79] Sultan, H., Rahman, S. U., Munir, F., Ali, A., Younas, S., & Khan, H. (2025). Institutional dynamics, innovation, and environmental outcomes: a panel NARDL analysis of BRICS nations. Environment, Development and Sustainability, 1-43.

[80] Hussain, M., Ahmed, H. A., Babar, M. Z., Ali, A., Shahzad, H. M., Rehman, S. U., ... & Alshahrani, A. M. (2025). An Enhanced Convolutional Neural Network (CNN) based P-EDR Mechanism for Diagnosis of Diabetic Retinopathy (DR) using Machine Learning. Engineering, Technology and Applied Science Research, 15(1), 19062-19067.

[81] Ramzan, M. S., Nasim, F., Ahmed, H. N., Farooq, U., Nawaz, M. S., Bukhari, S. K. H., & Khan, H. (2025). An Innovative Machine Learning based end-to-end Data Security Framework in Emerging Cloud Computing Databases and Integrated Paradigms: Analysis on Taxonomy, challenges, and Opportunities. Spectrum of engineering sciences, 3(2), 90-125.

[82] Hussain, S., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). An Enhanced Random Forest (ERF)-based Machine Learning Framework for Resampling, Prediction, and Classification of Mobile Applications using Textual Features. Engineering, Technology & Applied Science Research, 15(1), 19776-19781.

[83] Ahmad, I., Nasim, F., Khawaja, M. F., Naqvi, S. A. A., & Khan, H. (2025). Enhancing IoT Security and Services based on Generative Artificial Intelligence Techniques: A Systematic Analysis based on Emerging Threats, Challenges and future Directions. Spectrum of engineering sciences, 3(2), 1-25.

[84] Khan, H., Imtiaz, M. A., Siddique, H., Rana, M. T. A., Ali, A., Baig, M. Z., ... & Alsaawy, Y. (2025). An Enhanced Task Migration Technique Based on Convolutional Neural Network in Machine Learning Framework.

[85] Fawy, K. F., Rodriguez-Ortiz, G., Ali, A., Jadeja, Y., Khan, H., Pathak, P. K., ... & Rahman, J. U. (2025). Catalytic exploration metallic and nonmetallic nano-catalysts, properties, role in photoelectrochemistry for sustainable applications. Reviews in Inorganic Chemistry, (0).

[86] Liaqat, M. S., Sharif, N., Ali, A., Khan, H., Ahmed, H. N., & Khan, H. (2024). An Optimal Analysis of Cloud-based Secure Web Applications: A Systematic Exploration based on Emerging Threats, Pitfalls and Countermeasures. Spectrum of engineering sciences, 2(5), 427-457.

[87] Khawar, M. W., Salman, W., Shaheen, S., Shakil, A., Iftikhar, F., & Faisal, K. M. I. (2024). Investigating the most effective AI/ML-based strategies for predictive network maintenance to minimize downtime and enhance service reliability. Spectrum of Engineering Sciences, 2(4), 115-132.

[88] Ahmad, J., Salman, W., Amin, M., Ali, Z., & Shokat, S. (2024). A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. Spectrum of Engineering Sciences, 2(4), 133-149.

[89] Ayub, N., Ejaz, A., Hassan, B., Hussain, M. Z., Nadeem, M., Sabir, L., & Fatima, S. (2025). An Efficient Machine Learning And Deep Learning Based Deep Packet Security

Online ISSN 3007-3197
Print ISSN 3007-3189

Framework For Detection Of Computing Network Faults In The Iots. Spectrum of Engineering Sciences, 3(5), 659-674.

[90] Ayub, N., Imtiaz, M. A., Ali, E., Alqahtani, A. M., Ali, A., Ashurov, M., ... & Law, F. L. (2025). A Decision Framework for Intra Task Fixed Priority INTEL PXA270 Distributed Architecture for Soft RT-Applications Based on Deep Learning. Engineering, Technology & Applied Science Research, 15(3), 23553-23558.

[91] Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

[92] Splunk Inc. State of Security 2024. 2024. Available online: https://www.splunk.com/en_us/form/state-of-security.html (accessed on 1 October 2024).

[93] Chapman, R. Ransomware Cases Increased by 73% in 2023 Showing Our Actions Have not Been Enough to Thwart the Threat. 2024. Available online: https://www.sans.org/blog/ransomware-cases-increased-greatly-in-2023/ (accessed on 3 October 2024).

[94] Ayub, N., Habib, Z., Bakhet, S., Riaz, S., Rizwan, S. M., Abid, M., ... & Khan, H. (2025). An Optimal Ai & Deep Learning Mechanism For Mitigating Hacking Threat Identification Using Secure Network Infrastructure Based On Linux And Software-Defined Network (Sdn). Spectrum of Engineering Sciences, 3(5), 675-687.

[95] Aslam, I., Tariq, W., Nasim, F., Khan, H., Khawaja, M. F., Ahmad, A., & Nawaz, M. S. (2025). A Robust Hybrid Machine Learning based Implications and Preventions of Social Media Blackmailing and Cyber bullying: A Systematic Approach.

[96] Whittaker, Z. The Biggest Data Breaches in 2024: 1 Billion Stolen Records and Rising. Available online: https://techcrunch.com/2024/08/12/2024-in-data-breaches-1-billion-stolen-records-and-rising/ (accessed on 6 October 2024).

[97] Greenberg, A. Medical-Targeted Ransomware Is Breaking Records After Change Healthcare's $22M Payout. 2024. Available online: https://www.wired.com/story/change-healthcare-22-million-payment-ransomware-spike/ (accessed on 6 October 2024).

[98] Smith, G. Ransomware Statistics for 2024: Latest Trends & Attack Methods. 2024. Available online: https://www.stationx.net/ransomware-statistics/ (accessed on 28 September 2024).

[99] Ayub, N., Anwer, M. A., Iqbal, A., Rizwan, S. M., Shahbaz, A., Abid, M. H., & Rafi, S. (2025). Enhanced ML Framework based on Artificial Neural Network for countermeasures of Data Protection and Network Vulnerabilities Detection in Industrial Internet of Things. Annual Methodological Archive Research Review, 3(5), 410-431.

[100] Ghabban, F.M.; Alfadli, I.M.; Ameerbakhsh, O.; AbuAli, A.N.; Al-Dhaqm, A.; Al-Khasawneh, M.A. Comparative analysis of network forensic tools and network forensics processes. In Proceedings of the 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Cameron Highlands, Malaysia, 15–17 June 2021; pp. 78–83. [Google Scholar]

[101] Breitinger, F.; Hilgert, J.N.; Hargreaves, C.; Sheppard, J.; Overdorf, R.; Scanlon, M. DFRWS EU 10-year review and future directions in Digital Forensic Research. Forensic Sci. Int. Digit. Investig. 2024, 48, 301685. [Google Scholar] [CrossRef]

[102] Nandita, G.; Munesh Chandra, T. Malicious host detection and classification in cloud forensics with DNN and SFLO approaches. Int. J. Syst. Assur. Eng. Manag. 2024, 15, 578–590.

[103] Ferrag, M.A.; Ndhlovu, M.; Tihanyi, N.; Cordeiro, L.C.; Debbah, M.; Lestable, T.;

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN
3007-3197

Print ISSN
3007-3189

Thandi, N.S. Revolutionizing cyber threat detection with large language models: A privacy-preserving bert-based lightweight model for iot/iiot devices. IEEE Access 2024, 12, 23733–23750.

[104] Akhtar, M. H., Ali, A., Ali, S., Nasim, F., Aziz, M. H., Khan, H., & Naqvi, S. A. A. (2025). A Novel Machine Learning Approach for Database Exploitation to Enhance Database Security: A Survey. Spectrum of Engineering Sciences, 3(2), 26-57.

[105] Jabeen, T., Mehmood, Y., Khan, H., Nasim, M.F. and Naqvi, S.A.A., 2025. Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), pp.143-161.

[106] Akhtar, M. H., Jabeen, T., Aziz, R., Amin, M. N., Rizwan, S. M., & Hamid, K. (2025). Intelligence based Self-Healing Network Design: An Automated Incident Response System for Troubleshooting of IoT Security Breaches. Annual Methodological Archive Research Review, 3(8).

[107] Akhtar, M. H., Ali, A., Ali, S., Nasim, F., Aziz, M. H., Khan, H., & Naqvi, S. A. A. (2025). A Novel Machine Learning Approach for Database Exploitation to Enhance Database Security: A Survey. Spectrum of Engineering Sciences, 3(2), 26-57.