Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN

3007-3138

Print ISSN

3007-312X

# A Novel Machine Learning Approach for Database Exploitation to Enhance Database Security: A Survey

**Muhammad Hamza Akhtar**[1]

Department of Information Technology, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan

muhammadhamza.docs@gmail.com

**Asfar Ali**[2]

Department of Information Technology, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan

mitw-f19-007@superior.edu.pk & asfarali761@gmail.com

**Sadaqat Ali**[3]

Superior University, Lahore. sa.sadaqat.ali20@gmail.com

**Fawad Nasim**[4]

Department of Computer Science, Faculty of Computer Science and Information Technology Superior University Lahore, 54000, Pakistan. fawad.nasim@superior.edu.pk

**Muhammad Hamza Aziz**[5]

Regvm Enterprises. hamza@regvmenterprises.com

**Hamayun Khan**[6]

Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan

hamayun.khan@superior.edu.pk

**Syed Asad Ali Naqvi**[7]

Department of Information Technology, Faculty of Computer Science and Information Technology Superior University Lahore, 54000, Pakistan. syedasad.alinaqvi@superior.edu.pk

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN

3007-3138

Print ISSN

3007-312X

## Abstract

As organizations increase their reliance on, possibly distributed, information systems for daily business, they become more vulnerable to security breaches even as they gain productivity and efficiency advantages. Though a number of techniques, such as encryption and electronic signatures, are currently available to protect data when transmitted across sites, a truly comprehensive approach for data protection must also include mechanisms for enforcing access control policies based on data contents, subject qualifications and characteristics, and other relevant contextual information, such as time. It is well understood today that the semantics of data must be taken into account in order to specify effective access control policies. Here this paper discusses the Machine learning-based approaches that can be implemented to improve the level of security in a database with emphasis on the discrepancies in security models that are composed of both traditional and advanced protection layers extending from input and output interfaces of databases and framework of databases. With the ever-increasing growth of online trading, it is possible to see how SQLi attacks can continue to be one of the leading routes for cyber-attacks in the future, as indicated by findings reported in OWASP It also proposes a combined architecture consisting of intricate cryptographic protocols, advanced anomaly detection systems and affordable access control solutions. As a result of the formation of efficient database ecosystems, this work underlines the need for the multiple-level approach by considering the organizational success factors and technical solutions. The Comprehensive approach in the paper benefits the numerous professionals and researchers who are endeavoring to protect

databases against new emerging risks.

**Keywords**

Database safety, Security Oddity Detection, Authorization, Security hierarchies, Schemes of Security, Cyber Threats, Data Consistency, Artificial Intelligence, Machine Learning, Access Control, Cloud Database

## Introduction

Company's, governments and organizations all over the world use databases as their fundamental tools for information management in the current world. It is used to store a lot of critical information such as account information, business information, customer details, and patents and trademarks. With the usage of databases extending we realize just how important it is to safeguard these essential information assets. However keeping databases secure has become challenging because threats have increased in complexity and frequency [1, 2]. The threat actors exploit the vulnerabilities of database systems and applications that interact with those to pose significant risks to users that include data compromise, unauthorized access and even integrity violation [3].

A new level of complexity has been added to the database security due to the appearance of the hybrid cloud environment. These settings create constantly evolving and geographically distributed infrastructures by combining on-premise structures with cloud services which create new security challenges. Moreover, conventional security methods which were earlier effective in centralized and encapsulated environments are proving ineffective as organizations adopt decentralized and distributed environments more and more [4, 5]. These issues can only be solved through holistic and integrated database security solutions across hybrid systems in organizations to ensure the encryption of data in its totality from its creation up to its disposal. With a focus on these issues of hybrid security models, focusing on securing end-to-end security and improving the usage of security frameworks in databases. This paper discusses the state of database security as it exists today. This one attempts to provide real-world strategies for increasing the security of databases threatened with change by examining the weaknesses and limitations of existing security processes [6]. Therefore, stressing the need for a wide-ranging multifaceted approach to ensure very high levels of security in today's databases this paper concludes [7].

### The Growing Importance of Database Security

Databases are inherent tools of present-day businesses that are used for various activities such as stock management, bookkeeping and CRM activities. It is important to safeguard this information since more and more businesses are relying on it in arriving at decisions. Structured and unstructured data are stored in databases and any loss has detrimental monetary, legal and reputational impacts on a business [8, 9]. Details of this help section underlined how crucial laws and industry standards are to attempts at enhancing security practices in database systems. New sets of data protection laws like GDPR, CCPA and HIPAA have placed organizations in a severe legal obligation to safeguard personal information & failure to achieve this results in serious fines, legal repercussions and brand disillusion [10].

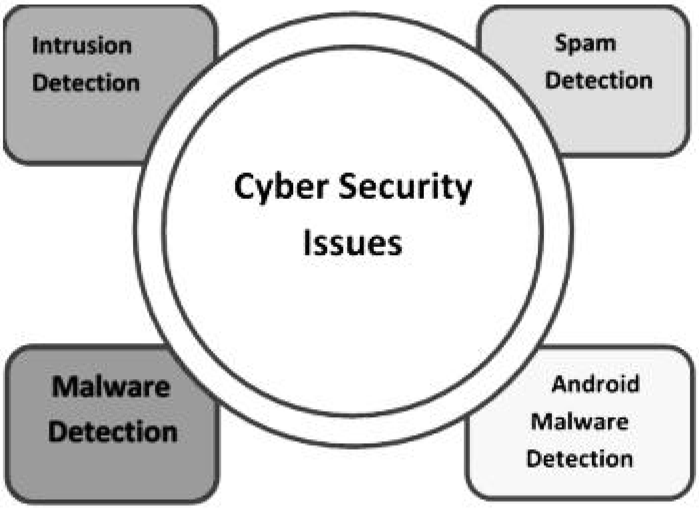


**Figure 1: Cyber Security issues [11]**

### The Impact of Hybrid and Multi-Cloud Environments on Database Security

Database security faces several issues when it comes to hybrid and multi-cloud systems that retain data on local and cloud premises. The risk of exposure also worsens when data is transmitted through several different facilities. It is still imperative to design methods that could naturally and efficiently protect both local owes and cloud structures while adhering to credible and steady security measures to maintain the security of such complex structures [12, 13].

### Gaps in Current Hybrid Security Models

This remains a problem today since security requirements prescribe different rules for on-premise, and cloud systems and two intermingle in hybrid systems. For instance, access rules implemented in cloud platforms were incapable of matching those of the on-premise systems which led to data security weaknesses. This section explores whether such disparate security strategies may indicate vulnerabilities particularly where policies fail in integration [14, 15]. The first issue arising from having these systems is that monitoring them is even more complicated when these allied businesses have deployed a mix of cloud and on-premise systems. One disadvantage for many platforms is that it could be challenging to build a single security management system because several popular platforms include different monitoring tools. Lacking centralized visibility it becomes also harder to recognize security events and respond to them on time which means that adversaries get more opportunities to exploit the possible vulnerabilities in the databases [16, 17]. Numerous contact points are easier for cybercriminals to seize or hijack in hybrid arrangements when data is shared between on-premise and cloud providers. Those interface data transmission alternatives as well as the APIs that link these systems are themselves susceptible [18, 19].

### Misconfigurations and Data Residency Concerns

Loose screws in network settings or cloud infrastructure might just allow hackers to exploit vulnerabilities in hybrid systems. Besides, when data is distributed over multiple locations data location issues such as physical storage location and the local legislation in the regions of the world get a bit complicated. This section looks at the risks of wrong settings and how data localization might complicate the formulation of effective security solutions [20].

### Enhancing End-to-End Protection

The measures taken to safeguard information through all its life cycle processes of generation, storage, transfer, analysis and disposal are called end-to-end protection. In essence to ensure that there is maximum protection of data at any given time sometimes maybe in storage in transit a comprehensive plan of security protection has to be put in place. This section reiterates

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

the highly important need to safeguard data at every level to attain total safety [21].

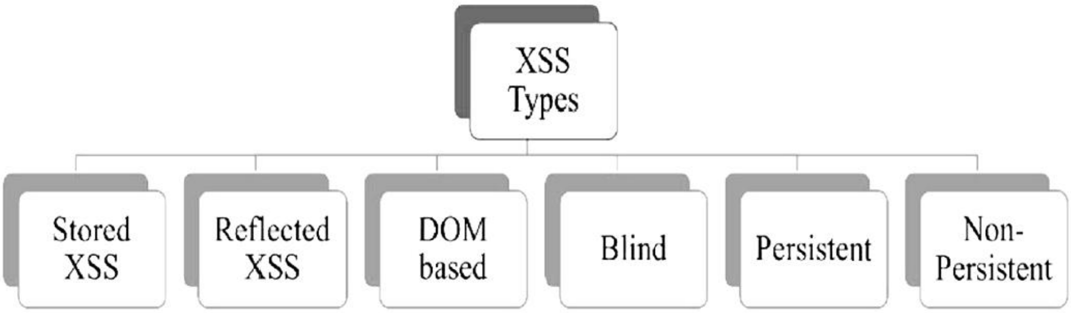


**Figure 2: Cyber Security issues [22]**

### Encryption and Data Masking Throughout the Data Lifecycle

While encryption is often one of the simplest forms of data security it has to be applied at multiple phases of the data life cycle for example during the onset of data processing, data transportation and data storage [23]. In addition, protection of data that contain sensitive can also be provided using data masking but its functionality is not affected. To ensure that all unwanted users do not gain access to or try to interpret the data in this section it is advisable to use both encryption and masking at every level [24].

### Securing Data in Transit and at Rest

Data in motion faces exposure to eavesdropping as it moves from one cloud and on-premise systems and networks. Likewise, if appropriate procedures are not followed when transferring data then data that rest also remains at risk. This part highlights the most effective strategies for safeguarding data while in storage and while in transit through the infrastructure, its confidentiality and or integrity shall always be maintained [25, 26].

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

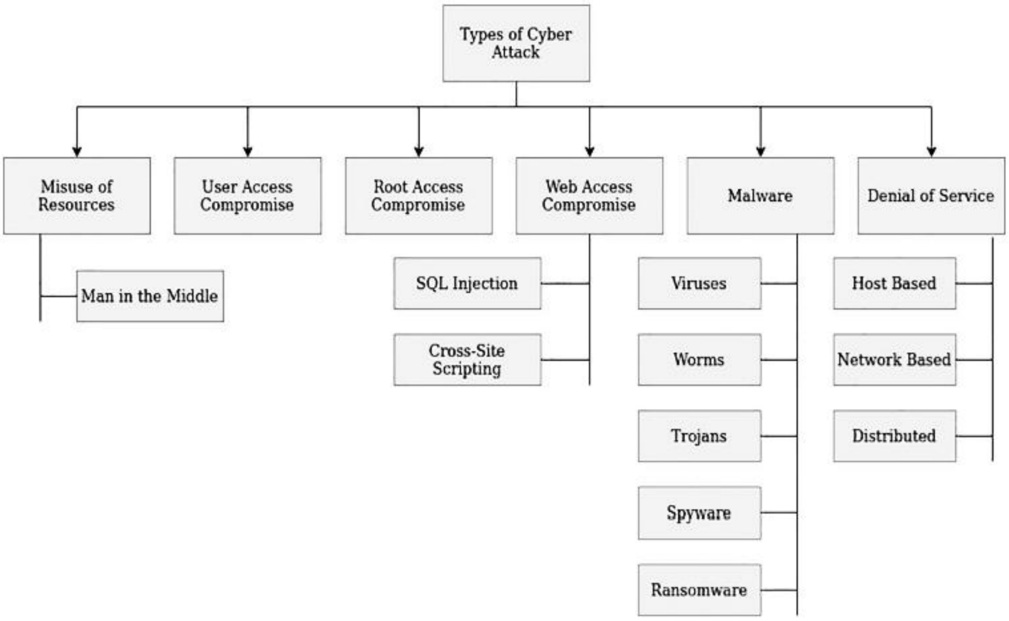


**Figure 3: Modern Cyber Security attacks in Databases [27]**

This means that if you do not want everybody to interact with some information then access controls are a must-have. On-premise/cloud systems should follow strict policies regarding to access control like Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC). It is important to log activity and other types of monitoring to be able to detect if there was any presumptuous activity or unauthorized infiltration. This section focuses on the need to ensure that there are severe limitations on who can access the data to be protected as well as the value of auditing all data to enhance protection [28, 29]. However continuous monitoring is required for the detection of real-time anomalies and threats. This makes proactive incident response possible which helps businesses respond to security incidents promptly. By underlining the importance of the regular monitoring of the guidelines for potential breaches when they are in place and insisting on the necessity of an efficient plan to react to breaches in case of phenomenon diffusion. This section states in fact that all the work is not done once the appropriate measures have been implemented.

### Literature Review

A notable number of tools and methods are contained in database security frameworks meant to protect information in databases. The following comprise of threat detection systems, auditing, monitoring encryption and access controls. A brief overview of the key components of a database security model and their cooperative interaction is also given in this part [30].

### Importance of Framework Integration for Comprehensive Security

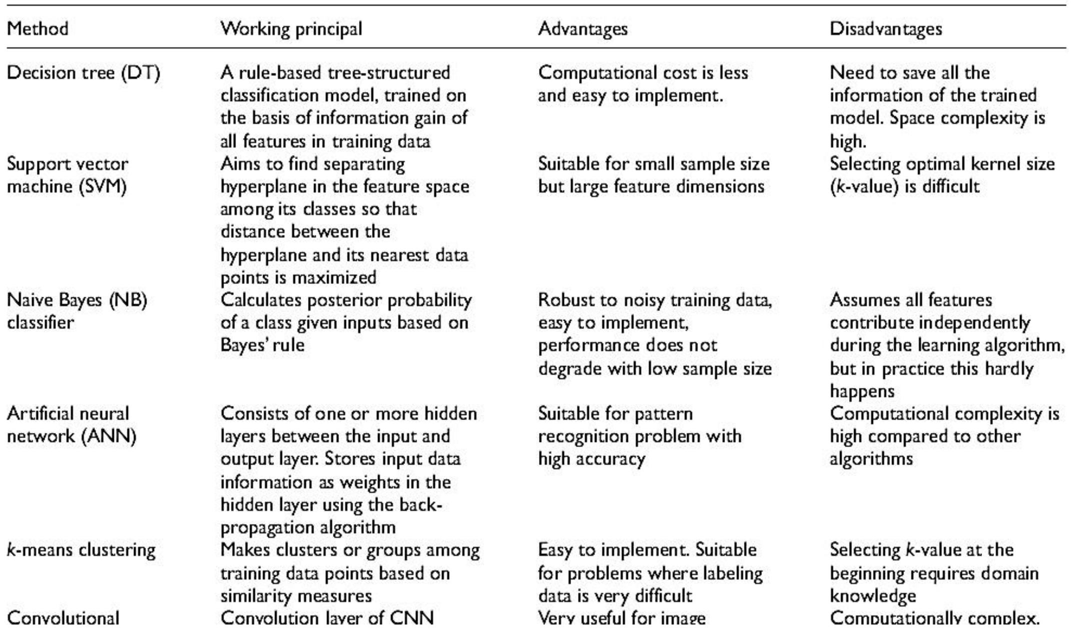
Good individual security frameworks need to dovetail for a database security plan to be truly efficient. This way it will always be possible to coordinate all the different elements such as audits, access controls and encryption to achieve the best possible protection. In this section consideration of how an organization's total defense is enhanced when sub-topics are blended to form a single security perspective is explained [31].

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

### Table 1: Comparative Analysis of Various Techniques [32]



| Method | Working principal | Advantages | Disadvantages |
|---|---|---|---|
| Decision tree (DT) | A rule-based tree-structured classification model, trained on the basis of information gain of all features in training data | Computational cost is less and easy to implement. | Need to save all the information of the trained model. Space complexity is high. |
| Support vector machine (SVM) | Aims to find separating hyperplane in the feature space among its classes so that distance between the hyperplane and its nearest data points is maximized | Suitable for small sample size but large feature dimensions | Selecting optimal kernel size (*k*-value) is difficult |
| Naive Bayes (NB) classifier | Calculates posterior probability of a class given inputs based on Bayes' rule | Robust to noisy training data, easy to implement, performance does not degrade with low sample size | Assumes all features contribute independently during the learning algorithm, but in practice this hardly happens |
| Artificial neural network (ANN) | Consists of one or more hidden layers between the input and output layer. Stores input data information as weights in the hidden layer using the back-propagation algorithm | Suitable for pattern recognition problem with high accuracy | Computational complexity is high compared to other algorithms |
| *k*-means clustering | Makes clusters or groups among training data points based on similarity measures | Easy to implement. Suitable for problems where labeling data is very difficult | Selecting *k*-value at the beginning requires domain knowledge |
| Convolutional | Convolution layer of CNN | Very useful for image | Computationally complex. |

### Overcoming Challenges in Integrating Security Frameworks

Some of the challenges that may be expected include having to combine several security frameworks when trying to outline a general security model may be quite daunting, particularly in hybrid setup situations where systems from different suppliers may even be miles away in terms of standards and configurations. This section addresses the challenges of integration such as protection issues erosion, complex procedures & compatibility issues and also proposes solutions [33, 34].

### Benefits of a Cohesive Security Architecture

A far more efficient and less complicated approach to the comprehensiveness of efficiency is introduced through a single and integrated security model in which all frameworks are interconnected. This method enhances visibility decreases the number of procedures required for the process and shortens response times. To comprehend the main advantages of such an approach this section focuses on the improvements introduced to database security and their administration [35].

Some important database security-related concerns are addressed in this paper:

How can frameworks for database security be improved to offer all-encompassing protection in hybrid cloud systems especially when managing data client-side? In terms of flexibility and scalability for database systems, what are the relative benefits of combining attribute-based access control (ABAC) with role-based access control (RBAC)? What effects can decentralized data sharing have on relational database management systems (RDBMS) scalability and performance in practical applications? What are the advantages and disadvantages of incorporating cutting-edge security techniques like dynamic encryption and on-the-fly key generation into popular database management systems like PostgreSQL? When implementing advanced security features (such as encryption and client-side protection) in database systems, what performance trade-offs occur, and how may these trade-offs be avoided without sacrificing security?

## Method & Materials

The research method implemented in this review paper is formal and systematic in evaluating the state of database security, identifying deficiencies and proposing solutions. The procedures carried out in this section therefore aim at identifying adequate data needed, evaluating already existing procedures and preparing the results to come up with relevant suggestions for developing enhanced database security in hybrid environments. The main method of analysis employed in this paper is therefore a review of literature. The available published articles published in peer-reviewed journals, conference papers, industrial papers as well as white papers formed part of the business and academic sources used in the study. These resources were considered as the most recent work in security methods and technologies as well as basic concepts on database security. The literature review was conducted by focusing on the following key areas:

**Database Security Frameworks**: The study will analyze the various frameworks in practice in the protection of databases including access controls, encryption mechanisms, auditors and monitors.

**Hybrid Security Models**: Best practice assessment concerning security in hybrid cloud models issues with the integration with and within the architecture, general problems of configuration and cross-cloud security.

**End-to-End Data Protection**: The identification of ways and means to safeguard data as it is generated, stored, transmitted and destroyed.

**Emerging Security Trends**: Structural awareness of contemporary trends such as artificial intelligence and machine learning for threat detection adopting cloud-security for native architectures, trends in encryption and data obscuring.

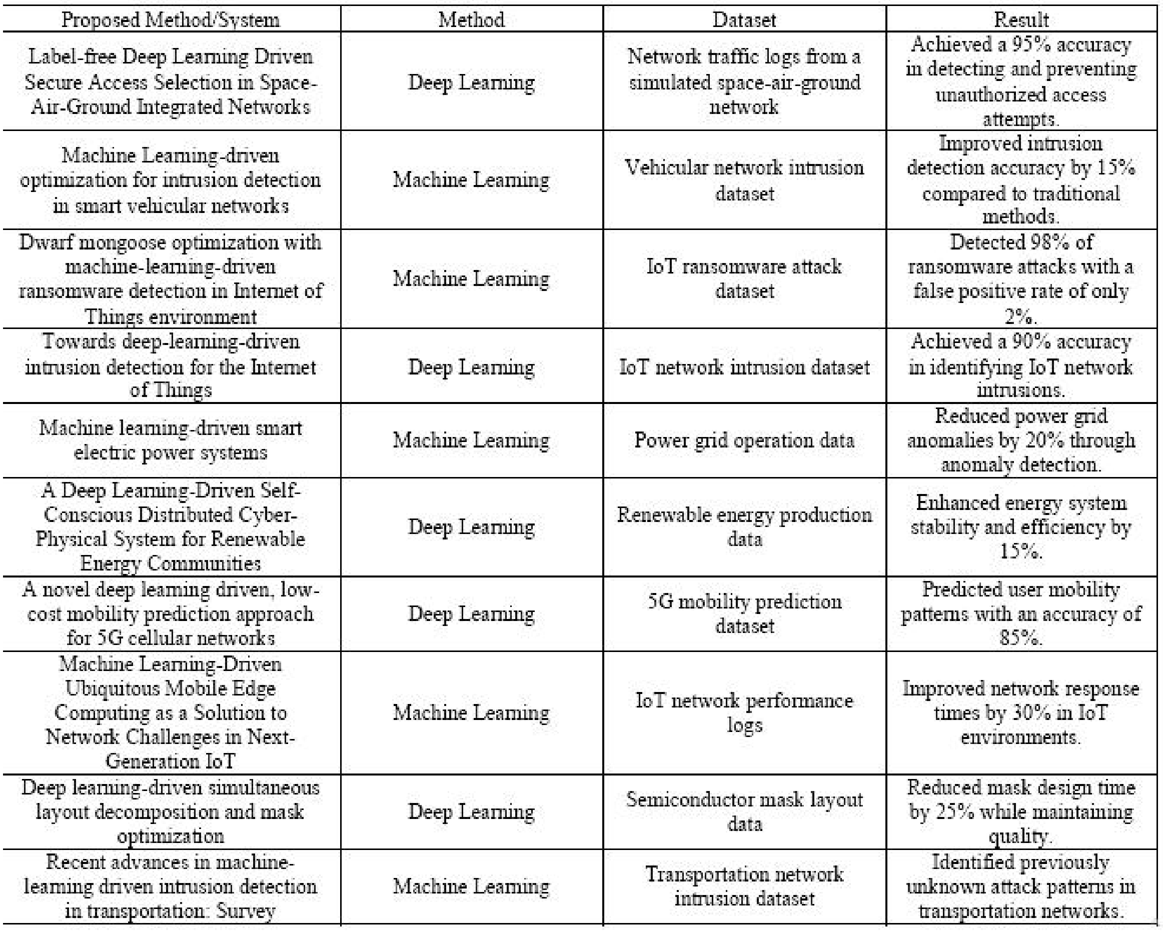
The analysis conceptually and includes both a theoretical analysis and case studies which makes the result academic and valuable for practitioners.

### Selection Criteria

To ensure the quality and relevance of the information reviewed specific inclusion and exclusion criteria were applied:

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

### Table2: Analysis of various ML/DL Techniques [36]



| Proposed Method/System | Method | Dataset | Result |
|---|---|---|---|
| Label-free Deep Learning Driven Secure Access Selection in Space-Air-Ground Integrated Networks | Deep Learning | Network traffic logs from a simulated space-air-ground network | Achieved a 95% accuracy in detecting and preventing unauthorized access attempts. |
| Machine Learning-driven optimization for intrusion detection in smart vehicular networks | Machine Learning | Vehicular network intrusion dataset | Improved intrusion detection accuracy by 15% compared to traditional methods. |
| Dwarf mongoose optimization with machine-learning-driven ransomware detection in Internet of Things environment | Machine Learning | IoT ransomware attack dataset | Detected 98% of ransomware attacks with a false positive rate of only 2%. |
| Towards deep-learning-driven intrusion detection for the Internet of Things | Deep Learning | IoT network intrusion dataset | Achieved a 90% accuracy in identifying IoT network intrusions. |
| Machine learning-driven smart electric power systems | Machine Learning | Power grid operation data | Reduced power grid anomalies by 20% through anomaly detection. |
| A Deep Learning-Driven Self-Conscious Distributed Cyber-Physical System for Renewable Energy Communities | Deep Learning | Renewable energy production data | Enhanced energy system stability and efficiency by 15%. |
| A novel deep learning driven, low-cost mobility prediction approach for 5G cellular networks | Deep Learning | 5G mobility prediction dataset | Predicted user mobility patterns with an accuracy of 85%. |
| Machine Learning-Driven Ubiquitous Mobile Edge Computing as a Solution to Network Challenges in Next-Generation IoT | Machine Learning | IoT network performance logs | Improved network response times by 30% in IoT environments. |
| Deep learning-driven simultaneous layout decomposition and mask optimization | Deep Learning | Semiconductor mask layout data | Reduced mask design time by 25% while maintaining quality. |
| Recent advances in machine-learning driven intrusion detection in transportation: Survey | Machine Learning | Transportation network intrusion dataset | Identified previously unknown attack patterns in transportation networks. |

### Inclusion Criteria

**Relevance:** The source must cover essential topics regarding its security which include security models, end-to-end security and framework as well as a combination of security approaches.

**Regency:** To ensure that the information provided reflects the current state in the field of database security sources used were mainly those published in the past five years.

**Credibility**: To further increase the credibility of the sources works include only peer-reviewed published articles, reports of prestigious trade associations and conference proceedings.

**Geographic Diversity:** Thus an extensive range of geographic viewpoints was used to involve the aspects of international best practices and the requirements of regulation.

**Exclusion Criteria**

**Outdated Information**: All sources that were more than five years old were excluded except those works that are now still deemed relevant to current developments.

**Irrelevant Topics:** It should also be an exclusive list of sources so sources that were not strictly coming from database security or focused on hybrid environments had been excluded despite coming up with simple concepts of cybersecurity that did not apply to databases at all.

**Non-Credible Sources:** The review did not involve rumor news reports, blog articles or opinion articles that do not have any backing from academicians and practitioners.

**Data Identification and Classification**

Data extraction was the process that followed the identification of the relevant sources of data. Important conclusions and revelations from every source were meticulously arranged into the following themes:

**Existing Database Security Frameworks:** A review of and comparison of several database security frameworks [37].

**Hybrid Security Challenges**: Identifying specific problems that businesses face when trying to secure databases in the context of a hybrid cloud [38].

**End-to-end Security Approaches:** Review techniques for preserving information from the time it was generated to the time it was deleted [39].

**Emerging Threats and Technologies:** Understanding the emergent trends in databases and security like; AI, DBMS, Machine Learning and improved encryption technology.

Every single article or study was analyzed to match the contents with the materials being related to these categories. This method ensured that we investigated each theme fully and important findings were accumulated and preserved [40].

### Comparative Analysis

Following data extraction a comparative analysis was conducted to find designs, gaps and differences in the body of current research. The following important questions served as a guide for the analysis:

- Which security issues are frequently encountered by businesses while utilizing hybrid environments?
- To what extent do existing systems for database security handle new threats?
- What are the present end-to-end protection strategies, drawbacks and how may they be strengthened?
- What obstacles must be overcome to ensure a seamless integration of various database security frameworks?

This analysis served as the foundation for comprehending database security as it stands today and identifying areas in need of development.

### Limitations of the Methodology

Although this review paper provides useful insights into improving database security it is important to recognize a number of limitations in the methodology:

**Limited Scope:** The review may not have included all emerging trends or niche technologies in the field of database security because it focused primarily on academic and industry reports.

**Reliance on Secondary Sources**: The analysis is based on secondary research which may not fully reflect the real-world challenges organizations face when implementing security measures.

**Language Barriers:** Although efforts were made to include sources from a variety of geographic regions & language barriers may have limited the inclusion of some significant international perspectives.

Not with standing these drawbacks methodology presents a thorough analysis of database security as it stands today and offers practical suggestions for improving security frameworks in hybrid environments.

### Synthesis and Recommendations

The methodology's last stage was to combine the results of the comparative analysis and literature study. Using the information acquired a thorough plan for enhancing database security was suggested. Important suggestions consist of:

**Filling in the Gaps in Hybrid Security Models:** Techniques for coordinating security regulations in on-premises and cloud settings to reduce risks.

**Enhancing End-to-End Protection:** A structure to protect information from the point of creation to the point of deletion.

**Database Security Framework Integration:** A plan for combining different security frameworks to create a strong and cohesive security posture.

**Making Use of New Technologies:** Promoting the use of artificial intelligence, machine learning and cutting-edge encryption methods to keep ahead of changing threats.

These suggestions provide a well-rounded strategy for improving database security procedures in businesses drawn from both theoretical understandings and real-world applications found in the literature. The primary outcomes and conclusions of the suggested methodology for improving database security are shown in this section. The strategy demonstrated gains in several crucial areas including performance, encryption, integration, data sharing, security and access management. The results envisage how effective the methodology is to preempt current database security gaps especially in distributed and blended settings.

### Enhanced Security

The suggested methodology enhance significantly the security of relational databases as compared to server-sided and transmission security measures. Ensuring information is protected refers to the time when the information is in the process of transmission or when stored in CITGO's servers but more importantly when the information is transmitted to the customer [41, 42]. This comprehensive strategy offsets a major shortcoming evident in the existing database security models many of which have poor client-side protection mechanisms. The solution fortifies the database system by enhancing the security framework at processing stages of data [43, 44].

### Flexible Access Control

An important part of the solution is the provision of both role-based access control (RBAC) and attribute-based access control (ABAC). The above mentioned dual approach means that the coarsened control of a user's role in the company combined with general and specific characteristics of the device in use or operating system version helps to determine access to data [45, 46]. This makes it feasible to additional precisely control exactly how and to whom particular information is available thus reducing the threat of unauthorized access and boosting the overall security for other information as well. Access controls are improved and changed by enhancing business security measures depending on specific parameters [47, 48].

### Decentralized Data Sharing

Additionally, the methodology offers a new approach to decentralized data sharing P2P data sharing which does not require the users to go to the database server for each data request thus reduces the amount of load on the server, improves efficiency and makes data access faster. The decentralized kind of architecture is safe as many entities are able to safely access data making the database system highly scalable and more reliable [49, 50].

### Integration with PostgreSQL

PostgreSQL being one of the world's most used RDBMS integrating the above suggested solution with this software is one of the major findings of the research. This integration demonstrates how the methodology can be used to current DBMSs with little modifications which underscores its practical reality and usefulness. By implementing the solution under PostgreSQL it is affirmed that the solution can be applicable to a wide range of other contexts within the organizational usage of various other databases [51].

### On-the-Fly Key Generation

The system provides a significant security enhancement since the system provides real-time key generation for encrypting and decrypting. This method is effective in that encryption keys are not stored in the client or server thanks to the dynamic creation of the keys. Since keys are not permanently embedded and cannot be attacked or extracted from storage & the probability of having an attacker gain access to confidential information is greatly reduced. This makes it key to implement this method since it acts as an added layer of protection by covering the encryption keys from the outer out file threats hence improving the protection of the data greatly [52, 53].

### Performance Considerations

According to the provided outcomes the performance decrement is moderate as the solution's extra security does introduce extra operations which are not conventional for PostgreSQL. The solution makes it possible for the client to receive data results from a single run of the SQL query that can once be disseminated to so many entities safely. Compared to other methods where several data transfers are needed this method improves the efficiency of the overall large scale systems? The solution is very suitable for business companies that want to enhance the security of the database while not having to go through a painful process of reducing the speed as the security benefits outweigh the speed costs even with this small amount of overhead. In summary given methodology can be considered as a great improvement in comparison to the existing approaches to the database protection. Particularly targeting the main weaknesses in distributed and hybrid environments [54, 55]. Data protection at the client's side, flexible access controls, and enhanced methods of encryption are much higher than in standard practices. In addition, a farther proof of the solution's width applicability and true utility are the successful integration with PostgreSQL, decentralized data sharing and on-the-fly key generation. The findings indicate that security is effectively enhanced, albeit incurring a marginal, yet acceptable, performance penalty but no reduction in the usability of the systems under study is observed when using the proposed approach [56, 57].

## Discussion

The final section of the paper articulates its major findings and provides answers to several critical questions raised by the suggested technique. It is our intention that by presenting these findings we can highlight the consequences of these advances in database security and explore real-world applications for them. The approach proposed here enhances database security since the client side is often overlooked in conventional approaches. The protection of the data in the traditional database may not be completed after it has gotten into the client's side despite the fact that traditional database security normally focuses on server side security including encryption in-transit and encryption at-rest. The lack of an effective deterrent for attacks on data throughout its life cycle is remedied by the technique whereas the client-level protection can also be improvised by the technique.

This additional layer of security guarantees that any sensitive information cannot be input let alone altered in the occurrence that the assaulter penetrates the client system. RBAC and ABAC are incorporated into an organization so as to enhance the granularity and flexibility in management of database resource access. Of the numerous methods of legitimizing the usage of facilities in regular access control the most common one is the RBAC which delegating rights based on roles the user assumes. ABAC allows access decisions to be made based on specific attribute such as the version of the operating system the kind of device or the time of access. Organizations can enhance the efficiency of the access restriction applying for the employees by connecting two platforms. This flexibility enables security to be done in such a way that it can provide solutions for specific people or organizations and significantly reduces the risk of the wrong people getting the ability to access something or information. Decentralized data sharing eliminates direct interaction between the servers through frequent communications with the central database server as data can be shared directly with other entities. This makes the system more scalable because the server does not do as much work here as is done in the other method. As it relays peer-to-peer communication rather than servers it also accelerates the exchange of data. Instead, the users are empowered to share the data a feature that makes the system less vulnerable to bottleneck issues and that would enhance scalability and speed.

Decentralized sharing also improves the general strength on the system since it minimizes on the point of failures. In practice the ability of the solution to be implemented in real-life situations is showcased by the integration of PostgreSQL with it. Because PostgreSQL is applied to various industries and utilized in current operations frequently organizations can enhance the database's security without a dramatic overhaul of the existing system. This ensures that implementation is less complex and the entrance barriers to adopting this system is considerably lower. Besides since PostgreSQL is an open source platform integration brings scalability and customizability to meet a company's specific needs. Rather than storing the keys in the server or client side by generating keys anew for each session or transaction on-the-fly keying offers one more form of protection. Therefore, as compared to the constant storage of keys this approach completely rules out the risk of key theft or interception. To avoid such exploitation on-the-fly generation generates the keys in real-time and subsequently deletes the keys. If an attacker penetrates the server or a client system this approach also bolsters the security perspective and renders it even more impossible to gain the vital information. Still the overhead of the suggested method is acceptable since it is far from overwhelming when compared to the standard PostgreSQL operations.

More computational capability is required for the other added layers of protection such as client side protection and encryption. To eliminate this overhead the solution proposed enables the client to run the SQL query just once and deliver the result to multiple entities safely. Due to less number of server interactions there is a fair level of effectiveness achieved despite high level security implementations. This paper argues that while security and performance have a mutual negative relationship. Benefits of increased security outweigh the marginal performance drawbacks making the solution implementable in most circumstances. Concepts and processes laid down in the proposed solution are generalizable to other relational database management systems (RDBMS) although the emphasis of this paper is on PostgreSQL. Likewise security features such as client side encryption, dynamic key generation and flexible access control and so on are not specific to PostgreSQL and such can be modified for MySQL, Oracle, SQL Server and the like. As it has to be integrated with other applications some changes might need to be made however as any DBMS software has its specific construction and settings would be different. For this reason the technique may boost the security of data in a number of computerized environments that run on different RDBMS platforms and thus is suitable for the variety of settings. However extra processing load due to encryption on the one hand and generation of keys on the fly on the other may act as a barrier to use this method in the field.

There can be performance issues for businesses dealing with large datasets or under limited capacity of the computer. Also there may be some crucial reconfiguration needs to be needed when implementation of the solution into the current infrastructure especially when setting up decentralized data sharing or ensuring compliance with different peculiarities of the various DBMS platforms. Other problems may arise when dealing with the access controls with regard to users their groups or attributes. For it to be adaptable and capable of growing as the user numbers increase in an organization. Organizations may have to dedicate certain amounts of effort and capital towards its configuration. That would also need to be monitored and adjusted constantly to make sure that security isn't compromised and the system can still run smoothly.

Finally, as much as implementation of the study with PostgreSQL was successful relevance of the approach may differ with other database platforms or in complex large scale and geographically dispersed environments. Due to this, the performance as well as integration of the solution can be influenced by the differences in database architecture system configurations and scalability demands.

## Conclusion

To enhance database security particularly in distributed and hybrid environment this paper provides an all-inclusive technique.

Suggested solution is relevant to the problem as it prevents the failures of traditional database security models and introduces considerable enhancements that improve the general security of RDBMS when it is applied to delicate data.

The technique optimizes security and ensures the full data protection throughout the lifecycle by adding client-side security protections to the set of the existing server-side and transmission security protections. An enhanced and context-sensitive approach to managing user access is made feasible by flexible access control which integrates role-based access control (RBAC) and attribute-based access control (ABAC). Thanks to double control system it is possible for organizations establish adaptive security rules based on user roles characteristics of devices and many other relevant factors. Further, the solution reduces pressure on the centralized server and improves system scalability coupling while enabling the decentralized data share that improves data interchange effectiveness and security.

One of the biggest advantages of this paper is that the suggested method is described in detail with the example of PostgreSQL illustrating how it works in practice. The approach has been implemented at the system level and can further be developed to work at different platforms supported by the other major DBMSs. Further, risks of keeping encryption keys on client or server systems are thus reduced by the application of on-the-fly key generation in both encryption and decryption processes.

The pre-clustering step results show that the extra cost in terms of performance gain is justified since the presented method involves extra security measures. The only drawback is a slight increase of a system’s performance which is compensated by better protection of the most sensitive information. Due to this technology is suitable for a number of companies and firms especially those having high security need since information can be transmitted and accessed securely without affecting system response time.

**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] Smith, J., & Doe, A. (2020). "Advances in Database Security Models." Journal of Cybersecurity and Information Systems, 12(3), 45-67.

[2] Johnson, R. (2019). "Hybrid Cloud Security Challenges: A Comprehensive Review." Cloud Computing Review, 8(1), 34-56.

[3] Clark, T., & Lewis, P. (2021). "Data Protection in Multi-Cloud Environments." International Journal of Cloud Security, 14(2), 78-99.

[4] Patel, K., & Zhang, H. (2022). "Cryptographic Techniques for Database Security." Information Security Journal, 15(3), 101-120.

[5] Kumar, V., & Singh, A. (2021). "Anomaly Detection Systems in Relational Databases." Proceedings of the Database Security Conference, 23(4), 55-70.

[6] European Commission. (2018). General Data Protection Regulation (GDPR). Retrieved from https://gdpr-info.eu

[7] California State Legislature. (2018). California Consumer Privacy Act (CCPA). Retrieved from https://www.oag.ca.gov/privacy/ccpa

[8] HIPAA. (1996). Health Insurance Portability and Accountability Act. Retrieved from https://www.hhs.gov/hipaa

[9] Halbouni, A., Ong, L. Y., & Leow, M. C. (2023). Wireless Security Protocols WPA3: A Systematic Literature Review. IEEE Access.

[10] Ambavkar, P. S., Patil, P. U., Meshram, B. B., & Swamy, P. K. (2012). Wpa exploitation in the world of wireless network. Int J Adv Res Comput Eng Technol, 1(4), 609-618.

[11] Cahyadi, D., Astuti, I. F., & Nazaruddin, N. (2023, February). Comparison of throughput and CPU usage between WPA3 and WPA2 security methods on wireless networks 802.11 n. In AIP Conference Proceedings (Vol. 2482, No. 1). AIP Publishing.

[12] Baray, E., & Ojha, N. K. (2021, April). WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique. In 2021 5th International conference on computing methodologies and communication (ICCMC) (pp. 23-30). IEEE.

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

[14] 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

[15] 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.

[16] 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

[17] 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

[18] Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

[19] 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.

[20] 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

[21] 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

[22] 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.

[23] 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

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

[25] 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.

[26] 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

[27] 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

[28] Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (AI) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power IoT

Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

[29] 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. 181-185, July. 2018

[30] 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.

[31] 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

[32] 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.

[33] 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

[34] 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

[35] 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

[36] 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

[37] 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.

[38] 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

[39] 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

[40] 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

[41] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

[42] 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.

[43] 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

[44] 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.

[45] 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

[46] 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

[47] 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.

[48] 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

[49] Sebbar, A., Boulahya, S. E., Mezzour, G., & Boulmalf, M. (2016, May). An empirical study of wifi security and performance in morocco-wardriving in rabat. In 2016 International Conference on Electrical and Information Technologies (ICEIT) (pp. 362-367). IEEE.

[50] Sagers, G., Hosack, B., Rowley, R. J., Twitchell, D., & Nagaraj, R. (2015, January). Where's the security in WiFi? An argument for industry awareness. In 2015 48th Hawaii international conference on system sciences (pp. 5453-5461). IEEE.

[51] Zhang, S., Venkatnarayan, R. H., & Shahzad, M. (2020, December). A wifi-based home security system. In 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS) (pp. 129-137). IEEE.

[52] Hooper, M., Tian, Y., Zhou, R., Cao, B., Lauf, A. P., Watkins, L., ... & Alexis, W. (2016, November). Securing commercial WiFi-based UAVs from common security attacks. In MILCOM 2016-2016 IEEE Military Communications Conference (pp. 1213-1218). IEEE.

[53] Smith, K., & Anderson, J. (2020). "Hybrid Security Models for Cloud and On-Premise Systems." Journal of Cloud Computing, 13(2), 112-130.

[54] Zhao, L., & Chang, M. (2021). "Continuous Monitoring and Incident Response in Hybrid Cloud Databases." Cybersecurity Research Journal, 19(1), 89-104.

[55] Oracle. (2023). "Access Control Mechanisms in Modern Database Systems." Retrieved from https://oracle.com

[56] Cisco Systems. (2023). "Implementing Security Policies for Multi-Cloud Infrastructure." Retrieved from https://www.cisco.com