# Enhancing Oracle Database Security: A Deep Dive into TDE, VPD, and Audit Vault Implementation

.

Harsha Vardhan Reddy Kavuluri[1*], Adithya Sirimalla[2]

[1*]Lead Database Administrator, Wissen Infotech Inc, USA. Email: kavuluri99@gmail.com
[2]Software Developer and DBA, 20755 Williamsport Pl suite 230, One Loudoun, VA, USA. Email: adithya.sirimalla@enliventech.net

***Abstract---*** Employee's commitment is an essential detail for organizational survival. Studies have demonstrated that commitment has a large effect at the successful overall performance of an organization. This is because an especially enthusiastic employee might be able to perceive with the dreams and values of the organization can have a more potent choice to belong to the employer and is willing to show more organizational dedication. If human assets are said to be an enterprise's greatest property, then devoted human assets need to be appeared as an agency's competitive benefit. Employee dedication complements process overall performance. A vital predictor of this type commitment is motivation, which motivates employees to spend time and electricity within the organization contributing to the success of the business enterprise. Because of this truth, there is a growing hobby in expertise the relationship between motivation and dedication. There is plenty of studies achieved at the topics involving motivation and dedication however studies on linkages among different varieties of motivation and exceptional attentions of commitment are hardly investigated. Factor evaluation, SEM which means structural Equation Modeling techniques is employed for information evaluation. The effects found that all extrinsic elements have effective and widespread effects on employees. This have a look at provides right quantity of knowledge at the significance of extrinsic factors for improving the personnel' commitment within the non-public commercial banks in Bangladesh.

***Keywords---*** Extrinsic Factors, Motivation, Private Commercial Banks, Employee Commitment, Bangladesh.

## I. INTRODUCTION

### 1.1. Importance of Database Security

IT is crucial to guarantee data confidentiality and avoid unauthorized access to the database. Since data is now stored in databases, the security of such data is crucial due to the surge of cybercriminals. [1-4] Here is a list of seven aspects showing why database security should be considered as the top priority: (Figure 1)


Figure 1- Importance of Database Security

Protection of Sensitive Data: The database contains sensitive information usually sensitive to the owner or any third party interested in it, for example, personnel records, account details, patient data, and other business information. The problem with this type of information is that it is not secure from theft, misuse, or exposure. Anti-virus programs, passwords, etc., or any other mechanisms that provide security to the information, support security from accessing information from unauthorized hackers.

Prevention of Unauthorized Access: One key factor that makes data vulnerable to losses is unauthorized access. In some cases, the attackers might find a way to breach the authentication by exploiting a weak or developed flaw in the configuration of a database system. By ensuring that RBAC, MFA, and strict and intensive passwords are applied, only the permitted people can make alterations to records in the database.

Compliance with Regulatory Standards: It is obligatory for companies engaged in data processing to follow legal requirements like GDPR, HIPAA, PCI-DSS, and SOX. They entail that companies use encryption, auditing, and limitations when accessing certain items. If it does not meet the compliance requirements, there are usually penalties that may be paid through fines, legal, or even damage to reputation.

Prevention of Data Manipulation and Integrity Attacks:

Protecting stored information is significant to provide the appropriate support for decision-making in the organization and other processes that require it. Malware may be used to perform an SQL injection, perform an inside attack, or manipulate the records of the database. Security measures, for instance, hashing, digital signatures, and transaction logging are also effective in ensuring data integrity since they prohibit alteration of data.

Mitigation of Cyber Threats and Attacks: These are essential because the databases are the major victims of cyber criminals currently using methods like SQL injection, ransomware, and Denial-Of-Service (DoS). Firewalls, intrusion detection systems, Database activity monitoring and automating threat response mechanisms lower the threat level of being attacked by intruders.

Business Continuity and Disaster Recovery: Security incidents such as leakage or theft of information are hazardous as they may paralyse organizational operations and result in beyond a loss. Measures like data mirroring and data protection in backup media, both on-site and offsite, help organizations to restore after potentially disastrous events like cyber intending, system breakdowns, or even accidental deletion.

Maintaining Customer Trust and Reputation: Most organisations have suffered the risk of a data breach, which can lead to loss of customer confidence and business deals, thus causing more damage. When it comes to database security, one cannot underestimate the need to protect customer information; this way, companies seek to prove they care for their customers, improving their B2C credibility.

### 1.2. Deep Dive into TDE, VPD, and Audit Vault Implementation

Transparent Data Encryption (TDE) Implementation: TDE is a feature used in the database for security purposes, and it concerns the encryption of data files in storage. This guarantees that TDE converts all the contents in the specific database files to unrecognizable codes that cannot be read without decryption keys, even with stolen files. It uses techniques such as symmetric encryption, including AES-256, but these do not slow down the performance of databases. The Oracle Key Management Framework (KMF) provides a way to manage keys to encrypt and decrypt the data so that only those users and applications who are allowed to decrypt the data are the only ones who can decrypt it. TDE is initiated through key stores' generation of keys and can be done at table or column levels. TDE works at the file level, which makes it function transparently to applications hence incurring small changes to the database queries; thus, TDE can be termed as a good supplement of security for compliance and data-sensitive organizations.

Virtual Private Database (VPD) Implementation: VPD stands for Virtual Private Database, and it is a type of access control method implemented by modifying a portion of the SQL query as per the user's rights. It differs from conventional access control systems that prevent users from accessing certain tables or databases completely VPD only allows them to observe or modify the rows and columns they want. This is particularly convenient in cases where many users are in the system, and everyone has different levels of privileges and data visibility privileges. VPD, in essence, involves the creation of policy functions in PL/SQL, which are associated with tables through security policies. The VPD policy allows the security conditions to be added to the SQL statement issued by a user, and the system removes prohibited rows from the results. While with the help of VPD, data confidentiality is improved and insider threat is prevented, there can be complications concerning policies that can slow down the query execution. Secure access to data is crucial in industries such as finance, healthcare, and government sectors, and VPD fits these sectors.

Audit Vault Implementation: Oracle Audit Vault is a technology that aids organizations in monitoring and auditing database activity to discover security threats and maintain compliance within an organization. It retains information on activity in several databases in real-time for analytics of access patterns, identification of violations, and production of compliance reports. The Audit Vault has three components: the Audit Vault Server, the collection agents, and the reporting console. The Audit Vault Server is designed to maintain the logs securely, and collection agents are used to get logs from different databases. It is up to administrators to set audit policy to determine the type of activity that needs to be audited, like, logins, permissions, and changes to data. After logs are obtained, the reporting console can be used to analyze the security, investigate the nature of events trends, and have a live monitoring of threats.

## II. LITERATURE SURVEY

### 2.1. Evolution of Database Security

Security of the databases has come a long way from basic levels of private controls to modern complex structures. In the beginning, protection was quite easy. A simple password protection of a database was used which can be easily cracked. [5-8] Several security controls emerged, such as data encryption, RBAC for managing users' access, and continuous auditing to monitor unauthorized activities. In the current generation, cyber security employs the use of machine learning and anomaly detection to facilitate the prevention of attacks.

### 2.2. Comparative Studies on Oracle Security Features

Quite many comparative studies have been carried out to determine the security features of Oracle against other DBMSs such as MySQL, PostgreSQL, and SQL Server. These studies show that Oracle has a comprehensive security solution, some of which include Transparency Data Encryption, Virtual Private Database, and Database Vault for containment of access. While most other DBMSs come with some basic security features, Oracle has tools for security as part of the database, and a company with high level security needs will find it more suitable for use.

### 2.3. Regulatory Compliance and Database Security

Due to increased concern regarding data protection laws

such as the GDPR, HIPAA, and PCI-DSS, enhancing an entity's security is crucial to meeting the regulatory requirements. Whether for regulatory compliance or feasibility, data encryption, access control techniques, and strict auditing procedures have become integrated values in adherence. Implementations of information security standards that require database security are meant to prevent liabilities and penalties. Thus, compliance-oriented security is a necessity for today's databases.

## III. METHODOLOGY

### 3.1. Implementation of TDE

#### 3.1.1. TDE Architecture

TDE is implemented to protect structured data by selecting data files for encryption so that personal data will not be easily available even when access to the physical media is gained. [9-12] TDE utilises symmetrical algorithms for data encryption purposes, including AES-256 encryption, while it does not hinder application operations. The key management within Oracle is achieved by a Key Management Framework (KMF) that includes auto login key stores and other things like a Hardware Security Module.

#### 3.1.2. Steps to Enable TDE

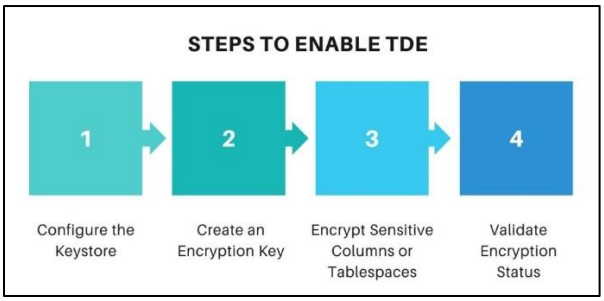


Figure 2 - Steps to Enable TDE

Configure the Keystore: One way to enable TDE is to create a Keystore, which manages all the encryption keys. There are many keystore types supported by Oracle – keystore based on software and Hardware Module Security Of Storage (HSM). Before continuing with the rest of the walk-through, there is an important step: create the Keystore, open it, and configure it so that the database can look for encryption keys when necessary. (Figure 2)

Create an Encryption Key: Once the keystore configuration is done, an encryption key is produced to encipher and decipher data in the database. Oracle provides an option for creating a master key for the database through the ADMINISTER KEY MANAGEMENT command. This key is a master key, the role of which is to guarantee the secure storage of information in the database platform.

Encrypt Sensitive Columns or Tablespaces: After generating the encryption key, specific database objects, such as the columns or even the tablespaces in the database, can be encrypted. Oracle TDE ensures adequate protection through details level encryption on one or more columns in a table or broad table space encryption. Encryption is, however, incorporated without interfering with the flow of the application and its interactions with the databases.

Validate Encryption Status: Once again, it is necessary to check its effectiveness whether encryption is enabled or not. The encryption statuses can be viewed by administrators from Oracle's Data Dictionary Views like Encryption_Keys & Dba_Encrypted_Columns to ensure that the data is encrypted securely. This paper also established that regular audits and key management practices ensure that the network remains secured with the need to adhere to various regulatory requirements.

### 3.2. Implementation of VPD

#### 3.2.1. VPD Policy Functions

VPD provides a high level of security through authorized row and column-level access by implementing policy functions. At the same time, it changes the SQL queries used based on login or session information to ensure that the user doesn't have access to unwanted data. It, therefore, increases privacy and security as only the authorized user can access the specific data, thus suitable for multi-tenant environments. For example, policy functions are in PL/SQL databases and provide dynamic predicates to be added to user queries to enhance filters.

#### 3.2.2. Creating a VPD Policy

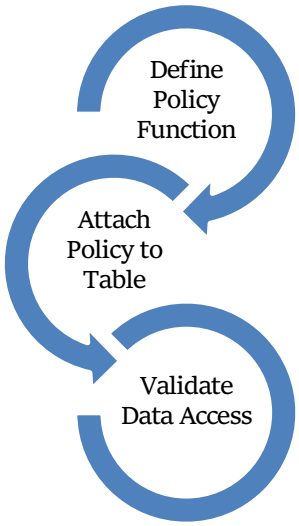


Figure 3 - Creating a VPD Policy

Define Policy Function: to execute this function, it is necessary to develop a policy function with PL/SQL to implement VPD. This function creates a dynamic WHERE statement to limit the data the application user can view based on the user's identity, the department, or any other parameter. It allows the user to view only the rows allowed to view, thus improving security and data privacy. (Figure 3)

Attach Policy to Table: After creating a policy function, it has to be associated with the database table using the procedure DBMS_RLS.ADD_POLICY. This links the function to the table and defines the instances when it should be implemented. This is because policies can be set in various SELECT, INSERT, UPDATE, and DELETE to cover all aspects of data security.

Validate Data Access: To verify, therefore, the effectiveness of the formulated VPD policy, the following steps should be taken after its implementation. IT professionals can test for multiple users to leave the firm's server to make certain restrictions implemented to accomplish the objectives. Trying to query data from the table using the various user accounts created should only allow access to the permitted data, thus ascertaining that the VPD policy is properly in place. Continual checks and modifications also ensure that security and policies are up-to-date regarding access control.

### 3.3. Implementation of Audit Vault

#### 3.3.1. Architecture and Components

Oracle Audit Vault is, therefore, a central control system for accumulating, storing, and managing audit trails from databases to improve security and compliance. The solution´s architecture consists of several components: collection agents, a repository database, and a reporting console. Like Check Point Certify, collection agents are located in database servers to collect compliance audit trails and transmit them to the Audit Vault Server, which will manage the received data. [13-16, 17, 18, 19, 20, 21] The reporting console enables the administrator to realize the audit activities, identify irregularities, and produce compliance reports. This arrangement makes the auditing real-time and assists organizations in avoiding any unlawful break-ins and leakages.

#### 3.3.2. Steps to Deploy Audit Vault

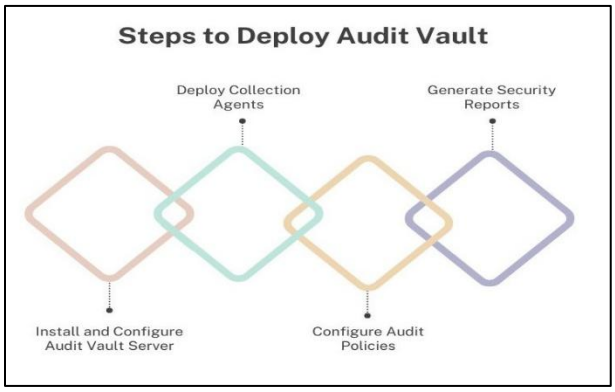


Figure 4 - Steps to Deploy Audit Vault

Install and Configure Audit Vault Server: The process starts with deploying Oracle Audit Vault Server on one specific machine to use solely for this purpose. This server is the focal reference system used to store audit logs. As such, it needs network parameters, storage space characteristics, and security measures inserted for efficient collection and protection of the logs. (Figure 4)

Deploy Collection Agents: After successfully establishing the server, the collection agents must be deployed on the servers hosting the target databases. They capture audit data from Oracle and other databases, applications, and systems in general. To allow communication only during data collection and concurrently after the agents are set up, they are registered with the Audit Vault Server.

Configure Audit Policies: After putting into practice collection agents, administrators establish audit policies that list the desirable log of activity in the database. The policies can be modified to alert in case of failed login attempts, data change, and privileges escalation. Further, the estimators meant to be fine-grained augment a tailored way of detecting the right events to make compliance and occurrence analysis efficient.

Generate Security Reports: Prepare the audit reports that will be used to study the security pattern to identify the potential threats. The Audit Vault offers stock and custom reports that simplify the investigation, compliance, and remediation of security incidents, if any. Additional protection is provided by the viewing, auditing and alerting where database activities are checked up consistently and automatically.

## IV. Results And Discussion

### 4.1. Performance Analysis

Transparent Data Encryption affects the performance of the database differently compared to a Virtual Private Database and Audit Vault. Table 1 outlines the above-mentioned security features based on three attributes: encryption overhead, query execution time, and audit log size.

Table 1: Performance Analysis

| Security Feature | Encryption Overhead | Query Execution Time | Audit Log Size |
|---|---|---|---|
| TDE | 50% | 10% | 0% |
| VPD | 20% | 80% | 0% |
| Audit Vault | 0% | 10% | 100% |

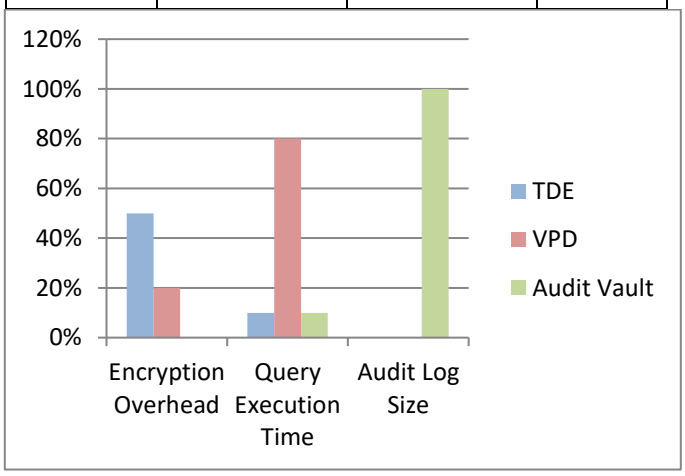


Figure 5 - Graph representing Performance Analysis

TDE (Transparent Data Encryption): TDE implies an additional factor of 50% as an encryption and decryption process consumes resources. However, the time consumer is reduced by only 10% for query execution time because while a query is being executed, the encryption is performed at the storage layer. Thus, it is not intrusive to database functionality. TDE does not write to any file and log mechanism. As such, there will not be any addition to the size of audit logs. From general prospects, TDE provides adequate security for data

stored in a database while not compromising the operation speed of queries. (Figure 5)

VPD (Virtual Private Database): VPD dynamically grants only fine-grained access control by adding the security predicates at the SQL level. This incurs an additional cost of 20% of policy evaluation, but the most affecting aspect of query execution cost is 80%. As the number of implemented security conditions increases, the time required to process the queries increases. As for some issues, VPD does not create logs as usual of an auditing system; therefore, it does not contribute to the size of the audit log. It may need performance tuning for large-scale policies, especially for row/column access control, which VPD is well suited for.

Audit Vault: The audit vault is aimed to maintain the data of audits and reports of audits in one location. However, it does not introduce intermediary encryption overheads, increasing the query response time by 10% as it logs security events in real-time. The impact is viewed with the greatest influence on audit log size because each activity in the database is logged for security review and compliance purposes, causing a 100% increase in size. Although this has the added advantage of improving security monitoring, organizations must provide enough storage for logs and think of archiving.

### 4.2. Security Enhancements

TDE, VPD, and Audit Vault together form a strong security system operating at multiple levels, which improves database security through the protection of data in the database, access control to the data, and development reports of all the activities. It is important as it encrypts data at the storage dimension to protect sensitive information. This way, even if the intruder gets physical access to the database files, he cannot decipher them without the keys. Having a transparent mechanism for operation, TDE does not infringe on the applications, making it ideal for the management of databases. Most importantly, it assists the organization in addressing the compliance issues of data protection laws like the EU GDPR, HIPAA, and PCI-DSS to retain data security from unauthorized access and breaches. VPD increases security by providing a multi-level data partitioning system per row and column of the database table. Unlike most systems that restrict access to all the tables or views, VPD dynamically changes the result set of SQL queries that are returned, making some parts invisible to the users based on roles, attributes, or policies that are defined. It also ensures that other users cannot access specific information with no privileged rights, leading to inside threats or leakage of sensitive information. Thus, VPD applies security policies at the database level and shall enhance sensitive information's security without requiring amplified alterations to application logic. However, complex policies may affect query performance, and these, therefore, ought to be well-optimized. Audit Vault also enhances security by offering more extensive auditing and monitoring qualities. It maintains audit trails that the supporting organizations can use to track all the activities in the database, including logins, changes, and unauthorized accesses. The centralized audit repository feature of Audit Vault enables the identification of irregularities, monitoring of suspect activities, and generating compliance reports aimed at conforming to laid down legal regulations. As with all the forensics frameworks, the vigilance and analysis of these responsibilities greatly minimize the risks involved by enhancing security within the database. Overall, using TDE, VPD, and Audit Vault together will enhance the security of an organisation's information to prevent unauthorized access and adhere to the latest regulatory standards.

### 4.3. Case Study: Securing Financial Transactions

The banking institution adopted TDE, VPD, and Audit Vaul to secure customer transactions and avoid the risk of unauthorized access.

Table 2: Case Study: Securing Financial Transactions

| Security Metric | Before Implementation | After Implementation | Change |
|---|---|---|---|
| Unauthorized Access Incidents | 100% | 60% | 40% |
| Data Breach Attempts | 100% | 40% | 60% |
| Compliance Violations | 100% | 30% | 70% |

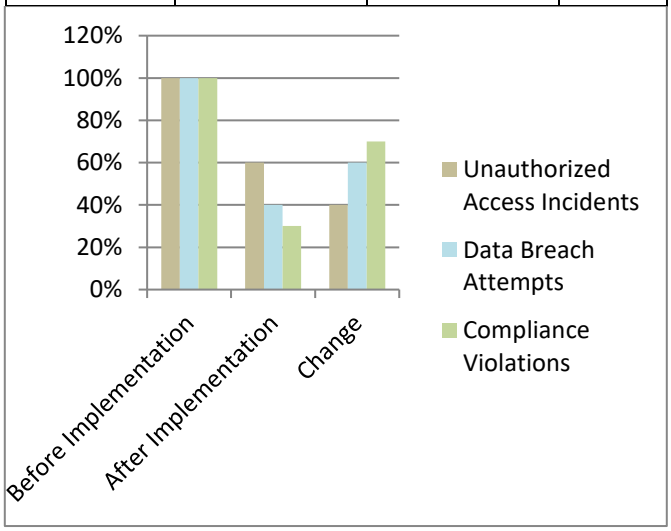


Figure 6 - Graph representing Case Study: Securing Financial Transactions

Unauthorized Access Incidents: Before taking all these measures, unauthorized access incidents were at a whopping 100 percent, which implies that there were several vulnerabilities within the organization through which unauthorized data access was always possible. Specifically, with the help of TDE, VPD, and Audit Vault, the number of cases of unauthorized access was minimized to 60 percent, which indicates that there has been improved by 40 percent. This decline shows that data encryption made it hard for unauthorized people to access important information, while fine-grained access control also inhibited unauthorized users, and auditing mechanisms provided the means of identifying and combating security threats. The organizations made many efforts to reduce cases of insider and external threats by

ensuring that only authorized personnel could access important data. (Figure 6)

Data Breach Attempts: The initial percentage of external or internal threats trying to breach the system's security was at 100%. Security postures improved, and subsequent breach attempts were only realized at 40%, and as such, the numbers were reduced by 60%. The implementation of TDE made it possible that even if attackers invaded the database, they could not read the encrypted information. VPD minimised access by users, especially those who were not supposed to access certain areas. Audit Vault provided real-time tracking of activities and even prevented them from escalating. This combination gave a strong security measure to reduce the leakage of vital data.

Compliance Violations: Lack of security policy, poor access control, and absence of audit procedures for regulating the organization's activities led to 100% of regulatory compliance violations. Security measures that were used helped reduce the compliance violations to 30 %, which marked an improvement of 70%. Using TDE in encryption ensured customer data complied with GDPR and PCI-DSS regulations, while VPD implemented access control to avoid data leakage. The main features that helped organizations ensure proper compliance within the auditing process include the logging and reporting frameworks that Audit Vault offers. This reduces the case of infringement of the set rules and regulations, improving overall compliance and avoidingf legal repercussions.

## V. CONCLUSION

This paper focuses on the key measures, namely TDE, VPD, and Audit Vault, that enhance the security of Oracle Database. This means that there are continuing challenges in how organizations can enhance data security and control access to meet the demands and standards set by the regulatory act, such as the GDPR, HIPAA, and the PCI-DSS. Incorporating TDE, VPD, and Audit vaults helps to achieve several layers of security that reduce risk exposures in unauthorized access, breach of data, and compliance issues. TDE is an important aspect of the solution that ensures that data is protected at the storage level by encrypting it. This means that even if some of the users sneak and gain access to the database files, they cannot decrypt or use the information inappropriately because they do not possess the relevant encryption keys. Due to high transparency, TDE does not interfere much with the existing applications; rather, it serves the legal need for  However, while TDE is beneficial in protecting data stored in the database, it does not facilitate control of access to the decrypted data, where VPD comes in to enhance security.

In addition, VPD offers precise access control by enforcing security in the row and even at the column level. Here, VPD works by changing the SQL queries generated and used by the OLTP according to the role and privilege level of the user. Thus, the unauthorized personnel cannot access confidential information, and the risk of insider threats is reduced significantly. While it is arguable that VPD can negatively affect the performance of queries, particularly when more policies are defined, it greatly improves the security of a multi-user database if the data restriction relates to the roles defined in the system. VPD allows rows and column-level security policies to be established to control the users' privileges properly. This is because VPD can change SQL queries according to the user's role and his or her permissions. This helps to bar any scrupulous person from accessing sensitive data and contain insider threats. While it is apparent that VPD may affect query response time, especially with an extensive policy, its capability to restrict data access by user role greatly boosts the database's security in a multi-user environment.

Yet another advantage of Audit Vault is its capability of giving detailed audit and continuous monitoring of the data base activities. It keeps a record of login attempts, data changes, and violations in access, which helps the security team to assess activities. The benefits of the identified approach would be manifold in general and include: In this way, organizations can create audit reports and discover emerging threats while they are still in their early stages. However, since the audit log file creates a huge file, managing storage and archiving the logs at intervals is critical for enhanced performance. In this case, TDE with VPD and Audit Vault makes sense as these are solid security solutions that help protect data from unauthorized access, maintain its integrity, and ensure it is always available. Although these technologies are impactful in enhancing security, there is a need to research more on security by AI, policy enforcement by AI, and AI-based anomaly detection. In the area of database security, the integration of AI and automation could lead to further increased effectiveness of threat detection in real-time, decrease the amount of time spent handling them manually, and improve the system's efficiency. In conclusion, one cannot overemphasize that cyber threats continue to grow in complexity; therefore, organizations need to update their security measures. Encryption, fine-grained access control, and auditing mechanisms are some of the existing ways databases can be secured; with the advancing technologies in both artificial intelligence and the automation of processes, new ways of even more secure database security are expected in the future enhanced digital world.

## REFERENCES

[1] Bertino, E., & Sandhu, R. (2005). Database security concepts, approaches, and challenges. IEEE Transactions on Dependable and Secure Computing, 2(1), 2-19.

[2] Kim, D., & Solomon, M. G. (2016). *Fundamentals of information systems security.* Jones & Bartlett Publishers.

[3] Schneier, B. (2007). Applied cryptography: *protocols, algorithms, and source code in C*. John Wiley & sons.

[4] Mousa, A., Karabatak, M., & Mustafa, T. (2020, June). Database security threats and challenges. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE.

[5] Alapati, S., & Kim, C. (2008). *Oracle Database 11g: New Features for DBAs and Developers*. Apress.

[6] de Alencar, M. S. (2022). *Cryptography and network security*. River Publishers.
[7] Protection, F. D. (2018). General data protection regulation (GDPR). *Intersoft Consulting, Accessed in October*, *24*(1).
[8] Act, A. (1996). Health insurance portability and accountability act of 1996. *Public law, 104*, 191.
[9] Mustafa, O., & Lockard, R. P. (2019). *Oracle Database Application Security*. Apress.
[10] Greenwald, R., Stackowiak, R., & Stern, J. (2013). *Oracle essentials: Oracle database 12c*. " O'Reilly Media, Inc.".
[11] How is data security maintained and what's new in Oracle 12c database security – Part 1, Red gate, online. https://www.red-gate.com/simple-talk/databases/oracle-databases/how-is-data-security-maintained-and-whats-new-in-oracle-12c-database-security-part-1/
[12] Tripathi, V., Agarwal, R., Pandey, P., & Kumar, S. A. (2019, March). Security Concerns in Data Warehouses: Implementation and Analysis of Virtual Private Database. In *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 117-120). IEEE.
[13] Bulusu, L. (2010). *Oracle embedded programming and application development*. CRC Press.
[14] JOkhakar, V. N., & Patel, S. V. (2010). Securing data warehouse using multidimensional modeling with a virtual private database. *National Journal of System and Information Technology, 3*(1), 1.
[15] Al-Breiki, H., Rehman, M. H. U., Salah, K., & Svetinovic, D. (2020). Trustworthy blockchain oracles: review, comparison, and open research challenges. *IEEE Access, 8*, 85675-85685.
[16] Database Security: A Technical Primer, Oracle, online. https://download.oracle.com/database/oracle-database-security-primer.pdf
[17] Natarajan, K., & Shaik, V. (2020, November). Transparent data encryption: comparative analysis and performance evaluation of Oracle databases. In *2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)* (pp. 137-142). IEEE.
[18] Haber, M. J., Chappell, B., & Hills, C. (2022). Regulatory compliance. In *Cloud attack vectors: Building effective cyber-defense strategies to protect cloud resources* (pp. 297-373). Berkeley, CA: Apress.
*[19]* Benaloh, J., Stark, P. B., & Teague, V. (2019). VAULT: Verifiable audits using limited transparency. *Proceedings of E-Vote ID.*
[20] Deshmukh, D. A. P., & Qureshi, D. R. (2013). Transparent Data Encryption--Solution for Security of Database Contents. *arXiv preprint arXiv:1303.0418*.
[21] Sidorov, V., & Ng, W. K. (2015, June). Transparent data encryption for data-in-use and data-at-rest in a cloud-based database-as-a-service solution. In *2015 IEEE World Congress on Services* (pp. 221-228). IEEE.