International Journal of Computer
Science and Engineering (IJCSE)
ISSN (P): 2278–9960; ISSN (E): 2278–9979
Vol. 11, Issue 2, Jul–Dec 2022; 179–198
© IASET

International Academy of Science,
Engineering and Technology
Connecting Researchers; Nurturing Innovations

IMPLEMENTING TRANSPARENT DATA ENCRYPTION (TDE) IN ORACLE DATABASES

Rakesh Jena[1], Nanda Kishore Gannamneni[2], Bipin Gajbhiye[3], Raghav Agarwal[4], Shalu Jain[5] & Prof. (Dr) Sangeet Vashishtha[6]

[1]Scholar, Biju Patnaik University of Technology, Rourkela, Bhubaneswar, Odisha, India

[2]Scholar, Nagarjuna University, ACWORTH, GA 30101, USA

[3]Scholar, Johns Hopkins University, Baltimore, MD, 21218, USA

[4]Independent Researcher, Mangal Pandey Nagar, Meerut (U.P.) India

[5]Research Independent Researcher, Maharaja Agrasen Himalayan Garhwal University, Pauri Garhwal, Uttarakhand, India

[6]IIMT University, Meerut, India

ABSTRACT

Transparent Data Encryption (TDE) is a robust security feature provided by Oracle Database that addresses the growing need for data protection in an era marked by increasing cyber threats and data breaches. As organizations amass vast amounts of sensitive data, ensuring its confidentiality both at rest and in transit has become paramount. TDE provides a seamless way to encrypt sensitive data without requiring changes to existing applications or workflows. This abstract explores the implementation of TDE in Oracle databases, detailing its architecture, operational mechanics, and best practices for successful deployment.

TDE operates at the storage level, encrypting database files and data blocks automatically. This means that data is encrypted before it is written to disk and decrypted when read into memory. The encryption keys used by TDE are stored in a secure location, separate from the encrypted data, ensuring that unauthorized access to the data is mitigated. The implementation of TDE in Oracle databases requires careful planning and consideration of various factors, such as performance impacts, key management, and compliance requirements.

One of the critical components of TDE is the use of encryption keys, which must be managed securely. Organizations must adopt a key management strategy that includes key generation, storage, rotation, and revocation. Oracle provides the Oracle Key Vault, a centralized key management solution that simplifies key management while enhancing security. This allows administrators to maintain control over encryption keys and comply with regulatory standards regarding data protection.

The implementation process involves several steps, including enabling TDE at the database level, configuring encryption for tablespaces, and managing encryption keys. It is crucial to test the performance implications of encryption and ensure that the database operations are not adversely affected. Regular audits and monitoring should also be conducted to assess the effectiveness of TDE and ensure compliance with organizational policies and regulatory requirements.

Moreover, organizations should also consider integrating TDE with other security features offered by Oracle, such as auditing and fine-grained access control. This holistic approach to data security helps organizations not only protect sensitive data but also strengthen their overall security posture.

In conclusion, the implementation of Transparent Data Encryption in Oracle databases is a vital step towards safeguarding sensitive information against unauthorized access and ensuring compliance with data protection regulations. As the threat landscape continues to evolve, adopting robust encryption strategies such as TDE becomes essential for organizations seeking to protect their data assets. By leveraging Oracle's TDE, organizations can achieve a balance between operational efficiency and data security, thus fostering trust and confidence among stakeholders.

KEYWORDS: *Transparent Data Encryption, TDE, Oracle Database, Data Protection, Encryption Keys, Key Management, Security Features, Compliance*

Article History

Received: 04 Oct 2022 | Revised: 08 Oct 2022 | Accepted: 21 Oct 2022