International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Developing and implementing advanced security protocols for safeguarding sensitive business data in SAP systems

Naresh Kumar Rapolu

Nareshkumar.rapolu@gmail.com

Abstract

The following research project has signified the development and implementation of advanced security protocols that are meant for designing to protect sensitive business data within the SAP systems. It has concentrated on effective risk assessment and vulnerability identification. At the same time, it has also been commemorated with stringent authentication and authorisation policies. Moreover, highlighting the relevance of data encryption and network security has been beneficial to protect information from getting tampered with. This has been attained by techniques such as multi-factor authentication and RBAC. Furthermore, it has incorporated appropriate encryption methods such as AES and TLS for the enhancement of data protection aspects within the organisations.

Keywords*:* SAP Systems, Risk Assessment, Identification of Vulnerabilities, Authentication and Authorisation Policies, Data Encryption, Network Security

1. INTRODUCTION

The research project will emulate a curated idea about the development and implementation of advanced security protocols. These protocols will be meant to safeguard sensitive business data within the SAP systems. It is termed to be evident in the present digital infrastructure where sensitive business data will have to be protected from cyber-attacks. It poses an essential concept for the organisation to safeguard their information before it can be tampered with. The research project will also allow proper risk assessment and vulnerability identification with stringent authentication and authorisation policies. Furthermore, it will also signify the role of data encryption and network security that will nurture positive outcomes in shielding the data from unauthorised access. This will lead to proper monitoring and compliance rules while ensuring the security and integrity of SAP systems and sensitive business data.

Figure 1: Advanced Security Protocols for Safeguarding Sensitive Business Data

2. Illustrating risk assessment and vulnerability identification for safeguarding sensitive business data in sap systems

Catering with a nuanced understanding of effective risk assessment and identifying the probable vulnerabilities are terms to be of paramount importance within the SAP systems. This is due to the fact that it proposes a detailed inventory of all the SAP applications and associated data. At the same time, this tends to analyse the assets and identify them for protection. Sometimes it is evident that the threat sources like external hackers and insider threats such as misconfigurations in the systems need to be evaluated carefully[1]. A suitable example states that vulnerability scanning has the tendency to explore the SAP BI reports which are accessible by more employees than necessary. This indicates excessive permissions. Moreover, the involvement of threat intelligence is considered to be useful in anticipation of potential attacks such as phishing campaigns. This entails targeting the SAP credentials. This is obtained by conducting penetration testing on a regular basis so as to simulate attack scenarios. As a result, this helps to predict the systemic weaknesses and thus nurtures valuable insights for curated remediation approaches[2]. This determines ethical protection of the sensitive data within the SAP systems therefore advantaging the organisations with sustainable outcomes.

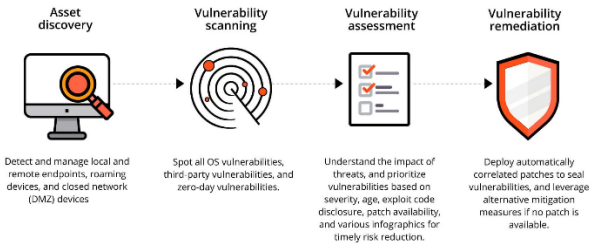

Figure 2: Depicting Vulnerability Scanning

3. Demonstrating authentication and authorisation protocols for accessing sensitive business data in SAP systems

Integration of authentication and authorisation are termed to be crucial in securing sensitive business data within the SAP systems. The reason behind this is that it stands to be an essential aspect in terms of preventing fraud. On one hand, authentication plays a significant role in verifying the user's identities before they get complete access to the SAP applications and services[3]. A suitable example replicates that the implementation of multi-factor authentication also abbreviated as "MFA" provides an extra layer of security which aids the users to deliver with a password and one-time code which are sent to their mobile devices. However, this tends to minimise the chances of risks related to unauthorised access. On the other hand, after the users are authenticated the role of authorisation comes into play. It has the tendency to control, their permissions within the systems. A sophisticated authorisation tool refers to Role-Based Access Controls also known as (RBAC)[4]. It assigns the users a specific role thus dictating the access

levels. Another notable example describes that a HR manager might have access to payroll information but lack permissions for viewing financial data. Thus, allowing regular views of the roles of the users and permissions results in compliance with organisational policies that help to detect security issues. This renders to protect the sensitive data in the SAP systems.

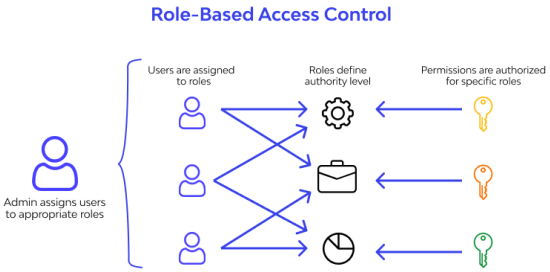

Figure 3: Understanding Role-Based Access Controls

4. Signifying the role of data encryption and network security

Data encryption and network security are identified to be two essential pillars for the development of security protocols in safeguarding sensitive business data in SAP systems. The first pillar which is data encryption is used in the case of implementation of end-to-end encryption which aligns that the data is protected both at rest and in transit[5]. A suitable example states that the utilisation of AES has been an effective medium for the encryption of database tables. This seeks to contain additional information about customers so that it prevents unauthorised access in the case of data breaches. However, the protection of data in transit is attained by the application of Transport Layer Security. It is nurtured with connections mapping SAP applications and users. This resulted in the successful establishment of data protection guidelines thereby limiting access to the encrypted data. This can be done by organising suits on a daily basis focusing mainly on encryption keys. As a result, this further maintained the sensitive data in the SAP systems. The second important pillar that is used to safeguard sensitive business data in eh SAP systems refers to network security[6]. It protects sensitive business data by developing a protected perimeter that helps to check the network traffic. It uses firewalls for the prevention of unauthorised access. In addition to this, it also utilises Intrusion Detection Systems for the identification of potential threats. A suitable example supports that by allowing robust configuration a firewall has the potential to block unwanted traffic thereby shielding against external attacks. It is evident that their remote employees can also access the SAP applications and services in a secure way without leading to potential risks[7]. This strengthens the network thereby gauging the organisations to respond to potential security risks and thus maintain data integrity.

Figure 4: Elucidating Data Encryption

5. Conclusion

This research project has exemplified the development and importation of advanced security protocols for safeguarding sensitive business data within the SAP systems. Concentrating on risk assessment along with identifying the vulnerabilities and authentication has been established with a stringent security framework. Additionally, the utilisation of authorisation policies followed by data encryption and network security has not only maintained compliance with the regularity standards but at the same time has also mitigated potential security threats and unauthorised access. Therefore, getting aligned with these curated security approaches has enabled the organisations to set the benchmark in protecting the confidential data resulting in successful data integrity and this prompting a secured segment for the sensitive data.

Abbreviations and Acronyms

- AES- Advanced Encryption Standards
- MFA- Multi-Factor Authentication
- RBAC- Role-Based Access Controls
- TLS- Transport Layer Security
- IDS- Intrusion Detection Systems

Units

- The data transmission rate is measured in bits per second
- Encryption Key Length is calculated in bits

Equations

- Data Transfer Time (TT) = [D / R], where D is the data size and R is the Data Transfer Rate
- Encryption Strength (ES) = [2^k], where k is the length of the encryption key

References

1. A. J. Trappey, C. V. Trappey, U. H. Govindarajan, J. J. Sun, and A. C. Chuang, *Ieee.org*,Oct.2016. https://ieeexplore.ieee.org/iel7/6287639/6514899/07600420.pdf

2. A. R. Naik and L. B. Damahe, "Enhancing Data Security and Access Control in Cloud Environment using Modified Attribute Based Encryption Mechanism," *International Journal of Computer Network and Information Security*, vol. 8, no. 10, pp. 53–60,Oct.2016,doi:https://doi.org/10.5815/ijcnis.2016.10.07

3. G. Seo, M. Sloan, S. Madnick, J. Maguire, and M. Cusumano, "Challenges in Implementing Enterprise Resource Planning (ERP) System in Large Organizations: Similarities and Differences

Between Corporate and University Environment ARCHNES Signature of Author," May 2013. Available:https://dspace.mit.edu/bitstream/handle/1721.1/80683/857768973-.pdf?sequence=2

4. M. T. Dlamini, J. H. P. Eloff, and M. M. Eloff, "Information security: The moving target," *Computers&Security*,vol.28,no.3–4,pp.189–198,May2009,doi: https://doi.org/10.1016/j.cose.2008.11.007

5. Q. Z. Sheng, X. Li, and S. Zeadally, "Enabling Next-Generation RFID Applications: Solutions and Challenges," *Computer*, vol. 41, no. 9, pp. 21–28, Sep. 2008,doi:https://doi.org/10.1109/mc.2008.386

6. S. S. Parimi, "Automated Risk Assessment in SAP Financial Modules through Machine Learning," *SSRN Electronic Journal*, Mar. 2019, doi: https://doi.org/10.2139/ssrn.4934897

7. T. Gutmann, D. Kanbach, and S. Seltman, "'Exploring the benefits of corporate accelerators: investigating the SAP Industry 4.0 Startup Program.' Problems and Perspectives in Management 17,no.3(2019):218.,"*Businessperspectives.org*,Aug.2019.https://www.businessperspectives.org/images/pdf/applications/publishing/templates/article/assets/12400/PPM_2019_03_Gutmann.pdf