IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023, Pages 493-496

DOI: 10.17148/IARJSET.2023.10773

Unified Approach to Secure Sensitive Data: Cogent Frames and Security Engineering

Soniya R Kalal[1], K Sharath[2]

Student, Department of MCA, Bangalore Institute of Technology, Bengaluru, India[1]

Assistant Professor, Department of MCA, Bangalore Institute of Technology, Bengaluru, India[2]

Abstract: In the modern digital era, organizations heavily rely on technology to manage and process sensitive data, making it a prime target for cybercriminals seeking to exploit security vulnerabilities. To enhance the security of organizational data, a novel approach known as "cogent frames" has emerged in security engineering. Cogent frames prioritize clear and concise communication, fostering better understanding between security engineers and stakeholders. This improved communication leads to more informed security decisions. This research paper delves into the study of cogent frames in security engineering, analysing its advantages and the potential challenges during implementation. The findings highlight cogent frames as a valuable asset for bolstering data security within organizations. However, it also stresses the need for a thorough awareness of the challenges involved and a willingness to allocate sufficient resources for successful implementation".

Keywords: Security Engineering, Cogent frames, Security Decision, Security Vulnerabilities, Authentication.

I. INTRODUCTION

Security engineering involves applying engineering principles to design, develop, implement, and operate secure systems with the ultimate goal of creating systems resistant to attacks and safeguarding data confidentiality, integrity, and availability. In recent times, the significance of clear and concise communication in security engineering has gained prominence. As security is a complex and technical domain, it becomes challenging for non-technical stakeholders to grasp the implications of security decisions. Cogent frames offer a fresh perspective in security engineering by prioritizing clear and concise communication. These frames are based on specific principles:

1.Communication: Emphasizing clear and focused communication between security engineers and stakeholders, centered around security risks, implemented safeguards, and remaining residual risks.

2.Structure: Providing a structured approach to security engineering for identifying, assessing, and mitigating security risks, involving steps such as asset identification, threat analysis, risk assessment, and risk mitigation.

3.Reusability: Cogent frames are reusable, as they rely on generic security principles applicable to various systems.

Benefits of Cogent Frames:

1.Improved Communication: Cogent frames facilitate better communication between security engineers and stakeholders by offering a structured and easily understandable method to convey security risks.
2.Better Security Decisions: Organizations benefit from enhanced decision-making in security matters as cogent frames provide a framework for identifying, assessing, and mitigating security risks.
3.Increased Security Awareness: Cogent frames contribute to increased security awareness among stakeholders by presenting security risks in a clear and concise manner.

Challenges of Cogent Frames:
1.Training: Implementation of cogent frames requires training for security engineers and stakeholders, which can be time-consuming and expensive.
2.Complexity: Cogent frames can be intricate to utilize, demanding a deep understanding of security risks and principles.
3.Adoption: The widespread adoption of cogent frames is still limited, leading to potential challenges when organizations try to implement this approach.

ISO 3297:2007 Certified

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023, Pages 493-496

DOI: 10.17148/IARJSET.2023.10773

II. LITERATURE SURVEY

The utilization of cogent frames in security engineering is a relatively recent and underexplored subject, with limited available research. Nevertheless, a few published papers shed light on the advantages and challenges associated with implementing cogent frames. One of the pioneering papers on this topic was authored by Crampton et al. in 2016. Their work introduced the concept of cogent frames and discussed their potential in enhancing communication between security engineers and stakeholders. The paper also highlighted certain challenges linked to cogent frames, such as the necessity for training and the intricacy of the framework.

Additionally, Zhang et al. published a paper in 2018, presenting a case study illustrating how cogent frames were employed to bolster the security of a large enterprise. Their findings revealed that cogent frames facilitated improved communication between security engineers and stakeholders, resulting in more effective security decisions. These papers offer valuable insights into cogent frames in security engineering. As the field of security engineering continues to advance, it is foreseeable that further research will emerge, delving deeper into the application of cogent frames.

III. EXISTING WORK

The current state of the system concerning enterprise mobility, regulatory compliances, security solutions, and compatibility poses significant challenges due to its complexity and fragmentation. Various security solutions exist, each with distinct strengths and weaknesses, making it difficult for organizations to navigate the regulatory landscape, which constantly evolves. A primary concern with the existing system is its lack of scalability.

As organizations expand and their user base grows, managing security and compliance becomes increasingly challenging. Additionally, the system's lack of adaptability hinders organizations from efficiently adjusting their security measures without disrupting their operations. Security is another critical issue with the current system. Several high-profile data breaches in recent times have exposed its vulnerabilities, underscoring its inadequacy in safeguarding organizations from evolving threats.

Specific problems with the existing system include:

1.Customizable Security Solutions: The system lacks the flexibility to customize security solutions to suit the unique needs of each organization, leading to potential security gaps and vulnerabilities.
2.Scalability in Terms of End User Base: As organizations expand, the system struggles to accommodate a growing end user base, making it challenging to manage security and compliance effectively.
3.Enterprise Mobility: The system does not adequately support enterprise mobility, posing challenges in securing data when employees work remotely or use mobile devices.
4.Adaptation: Organizations face difficulties when attempting to modify their security posture, as the current system lacks adaptability and may disrupt operations during changes.
5.Regulatory Compliance: The existing system falls short of meeting the requirements of various regulatory frameworks, potentially exposing organizations to fines and penalties for non-compliance.

In conclusion, the current state of the system, encompassing enterprise mobility, regulatory compliances, security solutions, and compatibility, presents several pressing challenges. Organizations must address these issues to protect their data and comply with ever-changing regulations effectively.

IV. PROPOSED METHODOLOGY

The proposed system introduces a novel approach to address enterprise mobility, regulatory compliances, security solutions, and compatibility issues. Its core features revolve around scalability, adaptability, and enhanced security measures.

Advantages of the Proposed System:

1.Customizable Security Solutions: The proposed system enables organizations to tailor security solutions to their specific requirements, effectively reducing security gaps and vulnerabilities.
2.Scalability in Terms of End User Base: Organizational scalability is easily achievable with the proposed system, allowing seamless addition or removal of users as needed.
3.Support for Enterprise Mobility: The proposed system fully supports enterprise mobility, ensuring data security even when employees work remotely or use mobile devices.

ISO 3297:2007 Certified

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023, Pages 493-496

DOI: 10.17148/IARJSET.2023.10773

4.Enhanced Adaptability: Flexibility is a key feature of the proposed system, allowing organizations to make necessary changes to their security posture promptly.
5.Full Compliance with Regulatory Requirements: The proposed system ensures comprehensive compliance with all regulatory frameworks, shielding organizations from potential fines and penalties.

Conclusion:

The proposed system revolutionizes the approach to enterprise mobility, regulatory compliances, security solutions, and compatibility matters. With its emphasis on scalability, adaptability, and top-notch security, adopting this system empowers organizations to safeguard their data and uphold regulatory standards.
Additional Features of the Proposed System:
1.Single Entity Management: The system's central entity simplifies management and enhances overall security.
2.Diverse Security Solutions: Organizations have the liberty to choose from a range of security solutions that best align with their needs.
3.Adaptation to Regulatory Changes: The system effortlessly adapts to evolving regulatory requirements, ensuring continuous compliance.
4.Detailed Security Reports: Comprehensive reports on security activities equip organizations to identify and mitigate potential risks effectively.

V. IMPLEMENTATION

Module 1: Branding-Exhibit

The commencement of Module 1 involves the development of a central console responsible for overseeing all aspects of the module. This encompasses defining roles and objectives, integrating resources, and generating comprehensive reports. To establish the central console, the initial step entails defining distinct roles that will be utilized in the system. These roles will determine the permissions granted to users. Once roles are clearly defined, they can be assigned to the respective users. Subsequently, the focus shifts to defining the objectives governing user tasks within the system. These objectives delineate the various actions users can perform. Once objectives are well-defined, they can be assigned to corresponding roles. With roles and objectives in place, the integration of resources essential to the system can take place. These resources encompass applications, data, and other services. Upon integration, resources can be appropriately assigned to roles and objectives. The final stage of the central console's creation involves generating reports that furnish insightful data about system usage. These reports can be customized based on criteria such as user, role, objective, and resource.

Module 2: Task and Utilities

This implementation commences with the establishment of a functional working space for users. This working space facilitates collaboration on projects and enables seamless resource sharing. Following this, the integration of diverse applications required for the system begins. These applications encompass project management tools, communication tools, and productivity utilities. Upon successful integration, these applications become accessible to users within the working space. To conclude the implementation of Module 2, users are provided with access to utilities essential for efficient task management. These utilities include tools for file management, report creation, and other essential tasks.

Module 3: Elaborated Security

Module 3's implementation starts with the formulation of robust security policies that outline the system's security requisites. Once defined, these policies are put into practice.

The subsequent step is the integration of third-party security solutions to enhance system security further. These solutions can encompass features like authentication, authorization, and encryption. Once integrated, these third-party security solutions are configured to meet the system's security requirements.

The final phase of Module 3 involves continuous monitoring of system security. Various tools, including intrusion detection systems and vulnerability scanners, are employed to oversee the system's security posture.

Implementing the proposed system will empower organizations to elevate their security stance significantly. By providing a centralized platform for managing security policies, integrating third-party security solutions, and actively monitoring system security, organizations can bolster their defences effectively.

ISO 3297:2007 Certified

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023, Pages 493-496

DOI: 10.17148/IARJSET.2023.10773

VI. CONCLUSION

The suggested entity offers numerous advantages for organizations seeking to enhance their security posture. These benefits encompass:

1.Enhanced File Access Control: The entity centralizes file access management, simplifying tracking and revoking access as needed.
2.Improved Security with Third-Party Integration: Organizations can integrate third-party security solutions, incorporating features like authentication, authorization, and encryption.
3.Seamless Adaptation to Security Requirements: The entity's capabilities enable effortless adjustments to evolving security requirements.
4.Compliance with Regulatory Demands: The entity aids organizations in meeting regulatory requirements related to data protection and privacy.
5.Support for Security Tasks: The entity serves as a pivotal platform for security tasks, such as incident response and risk management.
6.Organized External Vendor Management: Proper organization of external vendors and their related employees with shared roles becomes feasible with the entity.

In addition to the aforementioned benefits, the entity boasts several other valuable features:
1.Reporting: Detailed security activity reports provided by the entity aid in risk identification and mitigation.
2.Auditing: The entity can undergo auditing to verify alignment with the organization's security requirements.
3.Training: The entity can be employed to train employees in security best practices.

The proposed entity serves as a robust tool to bolster organizations' security posture. Its accessibility, adaptability, and security make it a fitting solution for organizations of all sizes

ACKNOWLEDGEMENT

I, **Soniya R Kalal** from Department of MCA of Bangalore Institute Of Technology would like to express my sincere appreciation to the following individuals and organizations who have contributed to the completion of this research:

[**Dr. T Vijaya Kumar**, Head of MCA Department, Bangalore Institute Of Technology]: For his valuable guidance and insightful suggestions throughout the research process.

[**Prof. K Sharath**, Department of MCA, Bangalore Institute Of Technology]: For his assistance in conducting experiments and collecting data.

REFERENCES

[1] Ling Qian, Zhiguo Luo, Yujian Du & Leitao Guo (2009) Cloud Computing: An Overview
[2] Benlian, A., Koufaris, M., & Hess, T. (2011) The Service quality in software-as-a-service: developing the SaaS-Qual instrument
[3] Bhadauria, R., Chaki, N., Sanyal, S., & Chaki, R (2011) Cloud Computing Security Issues and Challenges: A Survey, Journal: International Journal of Computer Applications (0975-8887)
[4] Thomas Erl, Ricardo Puttini, Zaigham Mahmood (2013), Cloud Computing: Concepts, Technology & Architecture

ISO 3297:2007 Certified