# Security Strategies for Safe Data and Content Access in Operational Modules of Product Data Management Software

Sam George[1] and K. David[2]

[1]*Research Scholar, School of Computer Science, Bharathiar University, Coimbatore, Tamilnadu, India*
[2]*Associate Professor, Department of Computer Science, H.H. The Rajahs College, Pudukkottai, Tamilnadu, India*
*E-mail: samtvmus@gmail.com*

Received 06 January 2018; Accepted 22 March 2018;
Publication 18 April 2018

## Abstract

In any engineering organisation, product data is dispersed across multiple departments which makes it vulnerable to unauthorised access. In the design of an automated system, enforcement of this access mechanism throws open the primary challenge in ensuring safety of each modules and the content inside. Challenges in security design initiates from the entry of users to the system. Security aspects for user access hold the key in safeguarding the content and data inside. However, management of this requires a holistic approach in letting the user traverse only through pre-defined modules, data categories with well-defined access mechanisms. Success of this modular security design will eventually lead to an efficient storage mechanism for the data inside and user friendly traversal and operational mechanism for the user.

**Keywords:** Authentication, Data, Log, Security.

*Journal of Cyber Security and Mobility, Vol. 7_1,* 87–94. *River Publishers*
doi: 10.13052/jcsm2245-1439.717

## 1 Introduction

Product Data in any manufacturing organisation is of high importance as it contains the entire knowledge covering the life cycle of the product. In this context security occupies high importance as any loss of this valuable information can prove fatal. Manufacturing organisation will have its entire knowledge repository spread over different verticals of an industry and this shall mostly be managed through network systems with stringent security measures. As such data management in a concurrent mode of operation calls for a detailed study on the configuration and operational aspects of data acquisition and operation in such a diverse engineering environment. The scope study imitates from understanding the individual aspects of engineering vertical existing in a central domain which is later converged to the system.

## 2 Security Domains in a Collaborative Environment

Ensuring security in a collaborative environment is always a matter of concern as it's not easy to detect the nature and source of attack. In this context, security design assumes significance as it's the available data which should be kept safe, rather than identifying and attacking the intruder. This context calls for identifying the nature of data which is preserved, the environment in which its kept, the possible source of intrusion that can occur, finally the remedial measures undertaken to avoid any data catastrophe. The security strategy for product data existing in a concurrent platform can be considered based on (i) Access Control and (ii) Content Level. Graphical depiction of a collaborative security design is shown in the Figure 1.

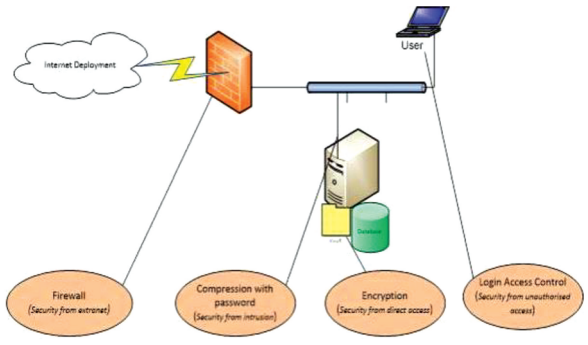


**Figure 1**

While access control restricts unauthorised access of information from a known source, Content security involves ensuring security on the existing data rather than being defensive. Both the strategies call for a synchronised approach in ensuring the overall data security.

## 2.1 Access Control

Access control is a method of permitting authorised data access with legitimate methods thus preventing intrusion. This can be further classified into (a) User level (b) Module level and (c) Document level.

### 2.1.1 User level access

This method controls user access through conventional login names and password. Each identified user in the system is given a unique login name and password which is designed with combinatorial sequence of alphabets, letters and special characters of identified length and complexity. Security in this design can be further strengthened with the number of attempts for login and a proper data repository mentioning the date, time and duration of system access. In its advanced strategy for a user level access, there can also be a provision to have the log recorded so that the same is traceable at any future time. To extend this further, an MIS system can be integrated with windows active directory security, so that in addition to enhanced security, it can offer single sign-on.

### 2.1.2 Module level security

In any knowledge based system, the vast storage of database repository gets visible through various modules of the system. In this context, module level security assigns security access to the various module where the data can be taken for manipulation. Information can be restricted to the users who are given legitimate permission to access those modules in an MIS system.

### 2.1.3 Document level

Document level security is one area of information security design where documents related to modules are saved with a unique identification parameter. This type of security is assigned against the category or genealogy under which each document is saved.

### 2.2 Content Level Security

While access control measures ensure proper security in data access from the visible and understandable sources, content security takes a defensive strategy to ensure that the data in its area of storage is kept safe. The various methods by which the content security is ensures includes (a) database level (b) vault level and (c) communication level.

#### 2.2.1 Database level

Critical information residing in the database can be secured by means of passwords and strong cypher encryption algorithms.

#### 2.2.2 Vault level

"Vault" is a disk folder where the document resides. Data in vault levels is kept in safe custody by means of encryption so that they remain protected and safe even if access directly through unscrupulous methods.

#### 2.2.3 Communication level

In a client server architecture model of data transport, the data in transit is safely transmitted using compressed passwords to prevent unauthorised access.

## 3 Design Strategies for Data Security in an Operational Environment

Basically, design strategies for data can be broadly classified as (i) Configurable Security and (ii) Operational Security. Configurable security assigns security to the core operations performed in the system and makes it mandatory to work in other operational modules of a system. Operational security of an MIS system provides operational rights on the modules where basic configurable security access has been set. This two-tier security access mechanism ensures access control facility in the system with basic access facility and operational facility.

### 3.1 Configurable Security Design

Configurable security facilitates the operational access to various features available in the system, by deciding individual access rights against each user or user group against module access. The advantage of providing such a

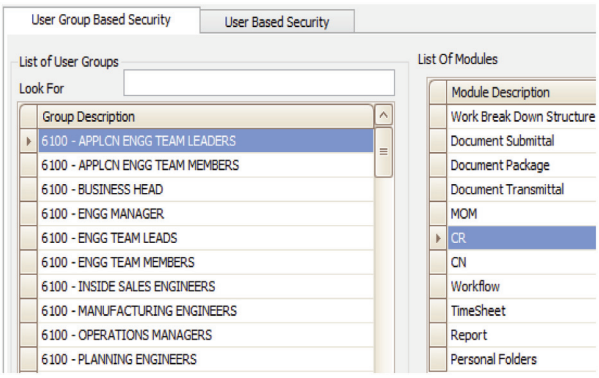


**Figure 2**

two – tier security is that only those users who are permitted to enter to the system and its operational modules only gets proper access. The configurable security design starts with identifying users under various user groups in a system then followed by module level security. The first and foremost access control facility is the user name and password for every individual user assigned to the system. Parameters involved can be made stringent with combinatoric iterations of symbols, letters and special characters. This security occupies prime importance as it's this identifications that goes anywhere when an audit of check is carried in modular operations. Security can be further be made stringent by assigning the validity period for the user name and keeping operational log records for later reference. The configurable security design extends to assigning modular rights where each user or members of a user groups shall only be permitted to access certain modules where they are legitimately bound to work. Design of modular specification is shown in Figure 2.

## 3.2 Operational Security

The first and foremost operational security strategy is to define various operations in a module where the user is entitled to operate. Operational Security ensures the access given to each user to perform individual operations on a module. This design aspect gets into assigning security modify, print to name a few. The various classification of operational rights in any module based on the category or genealogy is shown in Figure 3.

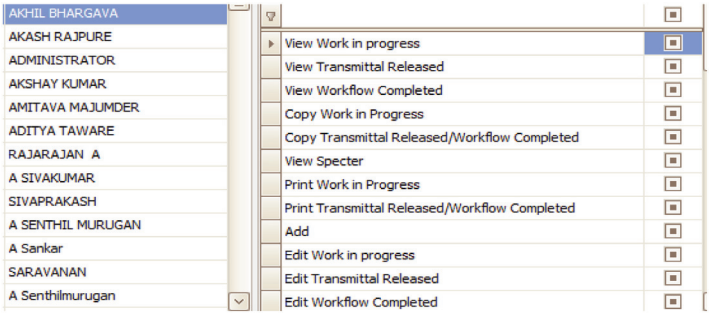


**Figure 3**

## 4 Implementation Analysis of Security in Workflow Design

Any mode of security design to be found successful and viable needs to be implemented in any of the modules in an MIS system. Workflow is one module in an MIS system which literally works in a concurrent environment connecting interdisciplinary departments. The security settings done in workflow assume great significance as this controls the live performance and movement of any object through it. Security design in workflow starts with identifying the resources who are authorised to operate on workflow design and its operational parameters. This includes the resources who are entitled to perform operations in each stage, the lead time that can be set for operation, checklists, sequencing of resources in each independent stage, bypassing or reversal of activities are some of the explicitly operations which can be performed on workflows. Operations performed during the workflow operations shall be logged for reference at any later stage. The operational stage of a workflow is shown in Figure 4.

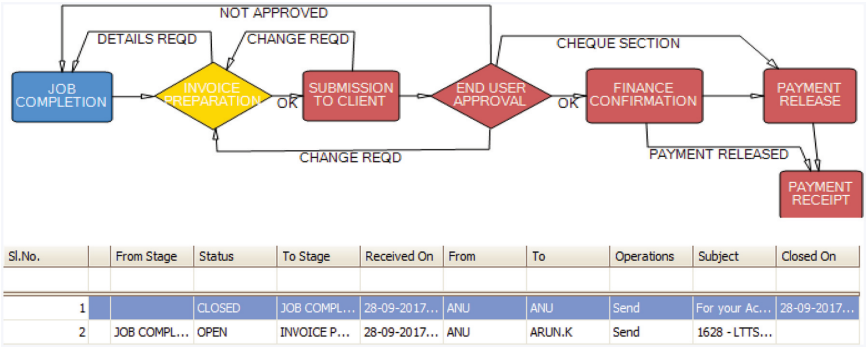


**Figure 4**

## 5 Scope for Further Study and Conclusion

Security design in a concurrent mode assumes much significance as this is one engineering domain which involves multi-disciplinary operations adhering to stringent network settings. The operational module holds challenges in setting up a secure system with utmost care in operational feasibility amidst stringent security constraints. Scope for further study and research in this area of domain points to security aspects on connection to multiple software's working in concurrence to produce a single output. Providing optimum output with the existing constraints with respect to multiplicity in terms of users, software's and systems poses the biggest challenge to be considered for further study and research.

## References

[1] Security design in WRENCH. Available at: www.wrenchsp.com
[2] George, S., and David, K. (2016). Workflow Enabled data Processing in a Concurrent Engineering Environment. *Procedia Technology*, *24*, 1643–1650.
[3] George, S., and David, K. An Ontological Approach for Product Data Management through workflow A Case Study Approach. *Journal of Computation in Biosciences and Engineering,* 2(3), 2348–7321.
[4] Sajan S. and Kunal. Working in WRENCH for BGR - PPX-0235 - 1 x 800 MW Dr. NTTPS BOP Project, Implementation Engineers, M/s. WRENCH Solutions. Available at: www.wrenchsp.com
[5] George, S., and David, K. (2015). Knowledge Management of Part and Bill of Material in an Engineering Industry. *International Journal of Applied Engineering Research,* 10(69).
[6] Tutorials on Concurrent Engineering Security for WRENCH. Available at: www.wrenchsp.com
[7] WRENCH tutorials. Available at: www.wrenchsp.com
[8] Ensuring security in concurrent mode for industries. Available at: www.wrenchsp.com

## Biographies

**Sam George** is a Research Scholar in Research & Development Centre, Bharathiar University, Coimbatore, Tamilnadu, India. After obtaining Degree in Mechanical Engineering from University of Madras, he has 12 years of experience as Domain Consultant in an organization of repute engaged in customized Engineering Data Management in the Product Life Cycle Management domain. His current areas of research include Knowledge Management, Concurrent Engineering and Product Data Management.

**K. David** is working as Asst. Professor, Department of Computer Science, HH The Rajahs College, Pudukkottai, Tamilnadu, India. He has over 15 years of teaching experience and about 4.5 years of Industry experience. He has published scores of papers in peer reviewed journals of national and international repute and is currently guiding 6 Ph.D scholars. His research interests include UML, OOAD, Knowledge Management, Web Services and Software Engineering.