Inter-Organizational Study of Access Control Security Measures

Winfred Yaokumah, Pentecost University College, Accra, Ghana
Eric Saviour Aryee Okai, Pentecost University College, Accra, Ghana

ABSTRACT

This study assesses the level of implementation and management of access control security measures among organizations. A survey was conducted and 233 responses were received from 56 organizations drawn from 5 major industry sectors of Ghana. This study focuses on the four access control clauses, namely access control policy, user access management, user responsibility and accountability, and system and application access control, which were adopted from ISO/IEC27002 international information systems security management standard. Overall, the results show that the organizations’ level of implementation and management of access control measures were approximately 66.6% (Level 3 - well defined), indicating that access control measures were documented, approved, and implemented organization-wide. Moreover, the results show significant differences in the implementation and management of access control measures among the organizations. For all the access control measures, the financial and health care institutions outperform educational institutions and government public services.

KEYWORDS


INTRODUCTION

Access control is the restriction of access rights to systems, applications, tasks, data, networks, and physical facilities (Mario & Andrea, 2014). It is a security feature that controls how users and systems communicate and interact with other systems and resources, with the intention of protecting information assets from unauthorized access (Harris, 2013). Data processing, transmission, and storage are carried out through the interaction among information systems components, consisting of people, hardware, software, procedures, processes, and communications facilities. These interactions should be managed and stringent measures ought to be implemented to prevent unauthorized entities from gaining access to critical and sensitive organizational information resources. Access control systems can manage the interactions and communications among users and systems (Ranjan & Somani, 2016). They can be effective in providing adequate security to information resources when correctly implemented and managed (Vaidya, 2010). However, implementing and managing access control measures are challenging tasks as systems administrators must deal with the rapid changes in business environment and also address various users with different levels of access rights requirements.

Access control management is a continuous activity of planning, controlling, coordinating, and organizing information security (Ngumbi, 2010). It is an area that is constantly changing in response to new threats, standards, and technologies (Jirasek, 2012). Access control requirements, implementation,
and management have become more challenging for organizations as a result of rapid developments in applications and systems, including cloud computing, Bring-Your-Own Device (BYOD), and the Internet of Things (IoT) (Lang & Schreiner, 2015). In order to deal with these challenges, organizations have deployed standard access control mechanisms, measures, models, technologies, and employed best practices. The processes and activities required to effectively implement and manage access control measures are detailed in ISO/IEC27002:2013, which is an information security management system. An information security management system (ISMS) comprises of the policies, procedures, guidelines, models, and related resources and activities that are collectively managed by an organization to protect its information resources (ISO/IEC 27000, 2014). Access control models are the frameworks that dictate how users access information resources. They consist of mandatory access control, discretionary access control, and role-based access control. Vaidya (2010) notes that though the discretionary and the role-based access control models have largely been implemented, most organizations perform permission assignments to users on ad-hoc basis and the permissions assigned to users are often poorly documented. This can lead to misconfigurations such as under privileges, violation of the least privilege requirement, and costly management of access control security measures (Vaidya, 2010).

Consequently, access control measures should be properly implemented and managed; otherwise, it can have significant operational impact on user productivity and the organization’s ability to perform to achieve its objectives (NISTIR, 2012). Despite its importance, few studies have been conducted in access control management in organizations. Mario and Andrea (2014) analyze information security literature of 1,588 papers from 23 information security journals and 5 conferences over the past four decades. The study suggests that future direction of information security research endeavour should focus on security management. Although several studies were conducted on the technical access control models and mechanisms (Karuppiah & Saravanan, 2014; Kayes, Han, & Colman, 2015; Ngo, Demchenko, & de Laat, 2016), few studies focused on management of access control measures.

Therefore, the purpose of this quantitative study is: (a) to determine the level of implementation and management of access control measures in Ghanaian organizations, and (b) to assess inter-organizational access control measures. To achieve this objective, the study focuses on the four access control management measures (access control policy, user access management, user responsibility and accountability, and system and application access control), which were identified by ISO/IEC27002 (2013). ISO/IEC 27002 is an international standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This widely-accepted document contains a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization’s information security (ISO/IEC 27000, 2014). To fulfill the research objective, the study answers the following research questions:

- To what extent is the access control security measures applied (implemented and managed) in Ghanaian organizations?
- Are there any significant differences among the organizations in their levels of access control security management?

The extent of implementation and management of access control measures may differ between organizations in developed and developing nations and even among organizations in the same country. Differences exist between organizations across the globe as a result of factors such as political systems, legislation, economic conditions, social and historical circumstances, and organizational culture (Abdullah & Valentine, 2009; Hofstede, 2001). Within a nation, the degree of implementation and management of access control measures may differ due to regulatory compliance requirements and the type of organization. A study in different environments and inter-organizational settings to evaluate the extent and the organizational differences in access control measures and management may provide significant findings. In particularly, an inter-organization study will provide information to benchmark performance of access control security measures and therefore foster competitiveness.
Interactive Design of 3D Dynamic Gesture Based on SVM-LSTM Model
www.igi-global.com/article/interactive-design-of-3d-dynamic-gesture-based-on-svm-lstm-model/207702?camid=4v1a