Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications

Journal homepage:
https://akademiabaru.com/submit/index.php/arca/index
ISSN: 2462-1927

Implementation of Malaysia E-government Information Leakage Protection Model

Hafizul Fahri Hanafi[1,*], Syarbaini Ahmad[2], Mohd Nawawi[3], Wan Azani Mustafa[4], Miharaini Md Ghani[5], Mohd Ekram Alhafis Hashim[6]

[1] Department of Computer Science and Digital Technology, Faculty of Computing Meta-Technology, Sultan Idris Educational University, Perak Malaysia
[2] Faculty of Creative Multimedia & Computing, Universiti Islam Selangor, Malaysia
[3] ICT Consulting Division, MAMPU, Malaysia
[4] Advanced Computing (AdvCOMP) Centre of Excellence, Universiti Malaysia Perlis, Malaysia
[5] School of Communication, University Sains Malaysia, Pulau Pinang, Malaysia
[6] Faculty of Arts, Sustainability and Creative Industry, Sultan Idris Educational University, Perak, Malaysia

ARTICLE INFO

Article history:
Received 20 February 2022
Received in revised form 28 April 2022
Accepted 30 May 2022
Available online 18 June 2022

Keywords:
E-government; Document security; Confidentiality; Information security; Digital document

ABSTRACT

The digital transformation of government management processes has ushered in an era of e-governance, leveraging digital technologies to enhance administrative efficiency. While this paradigm shift has brought numerous benefits, it has also exposed vulnerabilities, particularly in the realm of document security. Recognizing the need for innovation in this critical area, the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) developed the Malaysia E-Government Information Leakage model (MyEigle). This model introduces a Management Security System (MSS) method to mitigate the risk of confidential information leakage in official government documents. The document management model was tailored to align with Malaysian government sector workflows. A pilot study conducted among government servants in Putrajaya demonstrated improved document management practices and garnered positive feedback, suggesting the model's potential for enhancing security in e-government operations

1. Introduction

The Digital Era is a testament to human innovation and adaptability, an era where the boundaries between the physical and digital worlds blur. It empowers individuals and organizations alike to collaborate, learn, and innovate on an unprecedented scale. Yet, it calls for responsible stewardship of these digital tools to ensure they serve the greater good and do not exacerbate existing disparities. As we embrace the opportunities of this era, it is vital that we remain vigilant, ethical, and committed

[*] *Corresponding author.*
E-mail address: hafizul@meta.upsi.edu.my (Hafizul Fahri Hanafi)

to using technology as a force for positive change, steering the course of the Digital Era toward a brighter tomorrow.

However, the problem with the digital era is the threat to cyber security. The Digital Era has forced us to rethink traditional security paradigms. It's not merely about protecting physical assets but also safeguarding intangible digital assets, such as data, intellectual property, and confidential documents. The concept of security now extends to encryption, multi-factor authentication, and constant vigilance against emerging cyber threats. In this era, cybersecurity is not just a matter of individual responsibility but also a relationship between the government, corporate, and many more relations in global concerns.

The security issue with digitalization in e-government is tied to how it is managed. This is because the management method used will be a critical factor regarding the safety and effectiveness of using the digital document. In the administration of a government, this factor needs to be the focus of agencies to ensure that the benefits of digitalization are best taken in administrative affairs. Malaysia is one of the countries that prioritizes digital security in its governance. This was proven when it was recognized among the top ten countries that have the best cyber security systems in the world based on the Global Cybersecurity Index (GCI) [6]. One of the aspects of cyber security that are a concern in Malaysia’s e-government is the safety of documentation.

In the administration of government in Malaysia certain documents are classified as confidential and cannot be disclosed to the public. It is bound by Section 8 of the Official Secrets Act 1972 (Act 88) [2] which if convicted can be punished with imprisonment of not less than one year but not more than seven years. However, the leakage of official government secret information still occurs [1]. Some of the conditions that need to be paid attention to are the human factor, the change in technology, and the process and procedures of the document being managed. With the rapid innovation of digital and Internet of Things technology currently, the risk of information leakage is critical and risky since it can be done with just the convenience of at the tip of the finger.

To minimize the risk of leakage of confidential government information MAMPU the Malaysia Prime Minister's Department has taken the initiative to implement a project to protect the leakage of official secret information by using the Managed Security Service (MSS) method. This method has more of an e-government concept that digitizes confidential documents and is managed completely digitally, which is called MyEigle. This MyEigle project uses local ICT products to monitor and prevent the risk of leakage of official secret information at government servants whether received or sent through web server channels, social media, mobile storage, e-mail, and other smart devices. A series of them developed the Information Leakage Protection (DLP) framework, and the Bring Your Own Device (BYOD) implementation guidelines for Malaysia Government servants as an effort to prevent the leakage of information and confidential documents from being either due to human factors or the technology used.

This paper will discuss the relevant role and practices of MyEigle in detail. The combination of all the above-mentioned will then be modeled to become an effective digital document management process and meet the expected objective of reducing the risk of leaking information and confidential government documents.

2. Related Work

This study should be a high priority to be done considering the increase in leaks in government information management systems. The occurrence of the pandemic in 2020 and the ever-increasing use of digital technology add to the risk of leaking confidential information in the future.

To minimize potential information leakage, there are three methods proposed:

i. Data-in-storage (Data-in-storage/Data-at-rest) - inactive digital data stored in any digital form (database system, file system & various storage media)

ii. Data-in-movement (Data-in-motion) - digital data being transferred in the network (web browser)/ movement (via the Internet, wireless network & Malaysia Government servants' email)

iii. Data-in-use (Data-in-use) - digital data in use i.e., data that is being processed, deleted, accessed, or read (via desktop computer, laptop)

The implementation of information control methods is widely studied in several other countries as well. Among them are Estonia [3], Finland [4], and Sweden [5]. This method of information storage is not only implemented in government administration.

I.H. Montano *et al.,* [14] survey the existing techniques to protect against data leakage and to identify the methods used to address the insider threat. The study was concluded from 42 relevant papers from 2011 to 2022. The techniques involved in the study are intelligent documents, encryption, hash, virtual file system, biometrics, etc. The most popular technique used was encryption. But machine learning is growing as a trend lately.

Makarov and Shabunin [7] analyze Russian e-government development practices and some other countries. From the study, they proposed a policy based on PMI project management standards and IDEF0 standards as a methodology for public authority project management. They discovered the problem that the notation tools used were not enough to reflect all the business processes of the e-services for public authorities. So, they customize the methodology for the project management development with some extra elements (objects and subjects) designed to describe the process types and the corresponding e-services.

Patz [15] explores the case study of the European Commission in e-government and public administration in Europe. The discussion is purposely about leaking and leak prevention more broadly and analyses the efforts of the European Commission to prevent leaks. This is an empirical study of leaks and anti-leak measures in Western public administrations.

Abidin & Husin [8] begin the study with the weaknesses of the existing document management procedures in government organizations. After that new framework that integrates the implementation of the NFC system was proposed to suit current trends in communication. The study is based on Malaysia's e-government system with a focus on the security of a short-range communication, and the peer-to-peer communication capability in most mobile devices. It is mobile-based and suitable for Android mobile [16].

3. MyEigle Protection in the Public Sector

MyEigle is a protection model in public sectors that developed based on the experience that facing by government servants in working with various government sectors in Malaysia. It was developed to control the use of official government documents, and to avoid leaks of documents and information through document classification methods and effective management practices. It was implemented during the pandemic of Covid-19 period in Malaysia where most of the activities are executed in digital mode. It continues to be applied during the post-pandemic era partially until now.

i. Risk Management

Risk assessment activities must be carried out to ensure that all agency members who produce and handle official secret information are protected from the risk of information leakage. This list of civil servants is dynamic based on the duties and information handled.

ii. Change Management

Civil servants were found to be lacking in safe information-sharing methods as stipulated by the CGSO [9]. A comprehensive, periodic, and consistent training and awareness program should be implemented to build awareness and form a culture that emphasizes information security, especially involving the sharing and storage of official secret information. Wai [10] in Human factors in information leakage study suggests that the need to continuously train and remain where based on his research, most employees do not practice safe information-sharing methods.

iii. Process Owner

The process owner is the party responsible for information management in the agency. The owner of the process needs to be identified so that a comprehensive plan can be implemented to ensure the process of handling official secret information is orderly and meets the requirements of laws and regulations in force.

iv. Suitable Technology

To complete this study, the following elements need to be in high consideration.

a. Computer equipment

The use of computer equipment with a high capacity of random-access memory (RAM) and storage capacity of solid-state drive (SSD) is important to ensure that the process of detecting official secret information can be carried out in a suitable period, especially if the detection feature through optical character recognition (OCR) is activated.

b. Smart devices

The limitations of current technologies to monitor information leaks through Android and iOS devices cause many leaks to occur through personal Android and iOS devices. Furthermore, the implementation of BYOD is difficult to fully implement due to the lack of clear policies and policies regarding the use of BYOD by civil servants, visitors and contractors dealing with agencies.

c. Software and encryption storage

The Security Order enforces that it is necessary to implement encryption methods if it is necessary to bring out or share official secret documents with other parties. The use of storage or encryption software that meets the criteria set by the Security Order requires additional provision by MAMPU.

d. Information Filtering Software

The selection of content filtering applications by using appropriate information detection methods to detect the risk of leakage of official government secret information. The method used at government servants to detect the content of electronic documents against the risk of leakage is to use of content analysis, data fingerprinting, and regular expression methods as suggested by Alneyadi [11]. However, only some of the methods proposed are suitable to implement in this research.

v. Information Channel

By the current development of communication technology, all channels of information sharing such as email, instant messaging, mobile storage, and web browsers need to be monitored to ensure that official secret information is not shared illegally.

vi. Policy

The uncontrolled use of BYOD will cause networks, ICT systems, and government information to be exposed to the risk of spreading malicious code which in turn may cause information leakage. Adherence to the policy that has been outlined is very important in ensuring that this project can be implemented successfully. The Development and enforcement of BYOD and DLP policies and guidelines will reduce the risk of incidents of malicious code attacks and information leaks.

vii. Superior Support

a. Governance

The governance that includes the top management of the agency needs to be established. It is the key to effective monitoring and reporting actions that can be implemented to ensure that complete and effective planning can be organized toward creating an organization that is free from any information leakage.

b. Financial Support

Sufficient and reasonable financial allocations with initiatives made especially for the success of change management programs are important towards cultivating the right method of handling official secret information.

viii. Audit

The process of auditing against each violation of the rules set in the MyEigle needs to be implemented. It is very important as a regular reviewing process to look at the cause of non-compliance in the practice if any. Further action can be taken, and improvement will continuously be implemented.

4. Methodology

The methodology used in managing DLP is divided into the following categories:

- Monitor, detect, and enforce the protection of information leakage.
- Improving understanding and working culture in protecting official government confidential information among the government servants.
- General basic rules of classification of government documents and information.
- Pilot test

i. Monitor, detect, and enforce the protection of information leakage.

- MyEigle Framework was developed to monitor the implementation of DLP among government servants.
- DLP and BYOD policies, Guidelines, and SOP developed and used to monitor the implementation of DLP by targeting the goal of zero (0) leakage of Official Secret information.
- Monitoring of government documents and information leakage via dashboard according to the divisions involved.

ii. Improving understanding and working culture in protecting official government confidential information among government servants.

- Compliance culture so that 100% of government servants understand the SOPs developed.

iii. General basic rules of classification of government documents and information.

- Classification of the confidential level is stated in Table 1.

Table 1
Classification of confidential level

Keyword	Description	Case sensitive	Occurrence	Distance
RAHSIA BESAR	MAMPU RAHSIA BESAR *general keyword*	☑	2	0
RAHSIA	*MAMPU RAHSIA general keyword*	☑	2	0
SULIT	*MAMPU SULIT general keyword*	☑	2	0
TERHAD	*MAMPU TERHAD general keyword*	☑	2	0

- Change of pattern logic operator for basic rule features from Boolean AND to OR to obtain accuracy of rule violation detection.

iv. Pilot test

One Group Pre-test and Post-test design is used in this experiment to show that change occurs before and after treatment. Table 2 is the output from the experiment. It was recorded from January to October 2021. The cases noticeably increased during the pandemic since most government servants have been working at home start from Mei 2021. The pilot study is important because it helps researchers fine-tune the MyEigle model and identify potential issues or challenges before conducting a full-scale study. It also allows researchers to estimate the feasibility of this research and gather preliminary data.

4. Findings

Pilot users were given training and a series of workshops on the correct methods of handling classified government information throughout the project. The level of understanding of classified information handling procedures was measured at the beginning and the end of this pilot project. The results of this study will be supported by the number of rule violations detected by the MyEigle system. Respondents of the MyEigle pilot project were 200 MAMPU staff that were involved in the handling of classified information and were at risk of information leakage. The study was carried out for 10 months starting January 2021 with a trial period of 5 months and followed by enforcement of the DLP rules starting from June 2021 as stated in Table 2.

Table 2
Recorded Cases of Leakage in 2021

Month 2021	Violation Rules Cases	Total of Investigation	Real Incident
Jan	19	19	0
Feb	15	10	0
Mar	32	3	0
Apr	15	15	1
Mei	19	11	7
Jun	54	50	36
Jul	372	320	128
Aug	241	234	101
Sept	86	86	27
Oct.	88	87	19
Total	941	835	319

During the trial period, there were few non-compliances with the DLP rules detected as the detections were based on generic rules. The DLP rules were revised in June 2021 which resulted in improved detection of rule violations in July 2021 as shown in Figure 1.

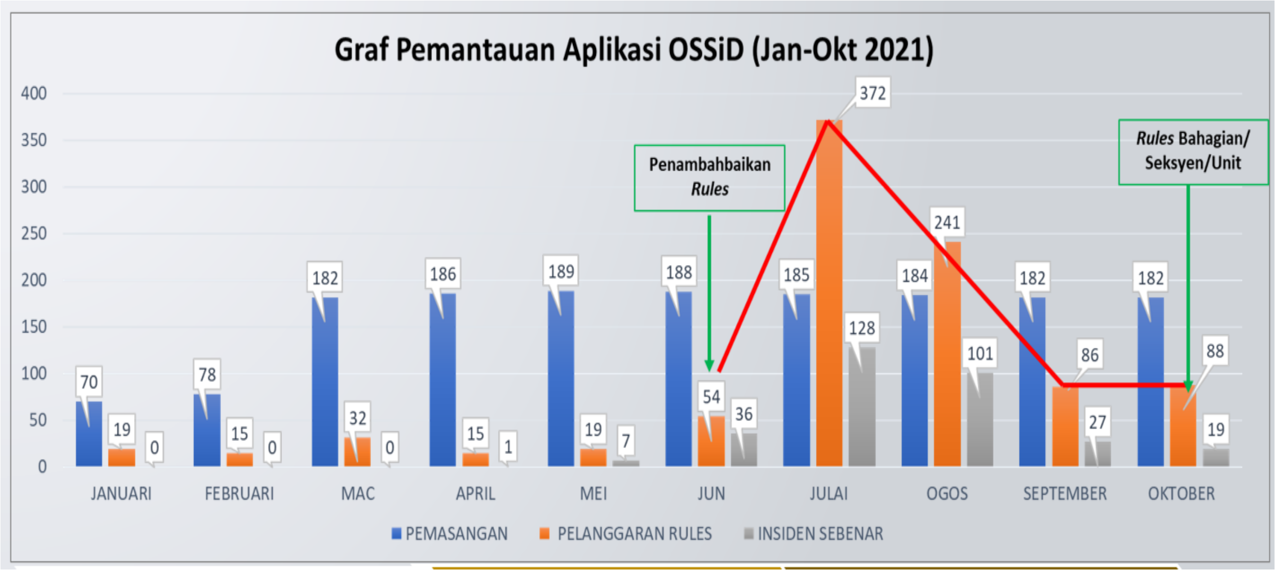

Fig. 1. Violations of DLP rules

Based on the number of rule collisions that were detected in July 2021 to September 2021, an investigation was conducted, and it was found that an average of 36 percent of the detections were real incidents. The DLP rules were further improved in September 2021 which resulted in the number of detected information leakage incidents being reduced to 26 percent.

Apart from improving DLP rules, personnel involved in DLP rule violations were given ongoing training and acculturation programs in handling classified information, which has reduced the number of DLP rules non-compliance detection.

4. Conclusion

In an era of rapid technological advancement, governments worldwide face the critical challenge of safeguarding sensitive information. The issue of information leakage, particularly concerning official state secrets in both physical and digital formats, remains a top priority for government agencies. While established instructions and regulations play a crucial role in mitigating risks, they alone cannot fully address the complex landscape of information security. The implementation of Information and Communication Technology (ICT) serves as a double-edged sword in this context. On one hand, ICT cannot completely prevent information breaches; on the other, it provides invaluable support in enforcing established security protocols. Advanced security measures such as encryption, multi-factor authentication, and intrusion detection systems significantly bolster data protection efforts. However, technology alone is insufficient to combat the multifaceted challenges of information security. A cornerstone of effective information security lies in the continuous education and acculturation of civil servants. Comprehensive training programs are essential to enhance awareness and develop crucial skills in handling sensitive government information. These initiatives should encompass a wide range of topics, including cybersecurity best practices, recognition of phishing attempts, and proper data handling procedures. By equipping civil servants with the necessary knowledge and skills, governments can create a human firewall against potential security threats. Moreover, the implementation of a holistic awareness management program for all civil servants is paramount. This initiative should focus on instilling correct information management practices, fostering a culture of security consciousness, and emphasizing personal responsibility in safeguarding government data. By cultivating a security-minded workforce, governments can significantly reduce the risk of inadvertent information leakage.

References

[1] mStar. 31 Kes Kebocoran Maklumat, Rahsia Rasmi Kerajaan. 14 Mar 2016.

[2] Undang-undang Malaysia, Akta 88 – Akta Rahsia Rasmi 1972 Pesuruhjaya Penyemak Undang-Undang Malaysia, Percetakan Nasional Malaysia Bhd. (2006).

[3] Stephany, Fabian. *It is not only size that matters: How unique is the Estonian e-governance success story?*. No. 15. Agenda Austria Working Paper, 2018.

[4] Lehto, Martti. "Cyber security education and research in the Finland's universities and universities of applied sciences." In *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*, pp. 248-267. IGI Global, 2018. https://doi.org/10.4018/978-1-5225-5634-3.ch015

[5] Sigholm, Johan, and Massimiliano Raciti. "Best-effort Data Leakage Prevention in inter-organizational tactical MANETs." In *MILCOM 2012-2012 IEEE Military Communications Conference*, pp. 1-7. IEEE, 2012. https://doi.org/10.1109/MILCOM.2012.6415755

[6] Statista. Countries with the highest commitment to cyber security based on the Global Cybersecurity Index (GCI) in 2020. Top countries GCI cyber security ranking 2020. Statista. (2020).

[7] Makarov, Anton, and Andrey Shabunin. "On design of secure E-Services for public authority in the russian federation." In *2017 20th Conference of Open Innovations Association (FRUCT)*, pp. 250-257. IEEE, 2017. https://doi.org/10.23919/FRUCT.2017.8071321

[8] Abidin, Siti Salbiah Zainal, and Mohd Heikal Husin. "Improving accessibility and security on document management system: A Malaysian case study." *Applied Computing and Informatics* 16, no. 1/2 (2018): 137-154. https://doi.org/10.1016/j.aci.2018.04.002

[9] Arahan Keselamatan (Semakan dan Pindaan 2017), Chief Government Security Office (CGSO), Prime Minister Department of Malaysia. 2017.

[10] Wong, Wai Peng, Hwee Chin Tan, Kim Hua Tan, and Ming-Lang Tseng. "Human factors in information leakage: mitigation strategies for information sharing integrity." *Industrial Management & Data Systems* 119, no. 6 (2019): 1242-1267. https://doi.org/10.1108/IMDS-12-2018-0546

[11] Alneyadi, Sultan, Elankayer Sithirasenan, and Vallipuram Muthukkumarasamy. "A survey on data leakage prevention systems." *Journal of Network and Computer Applications* 62 (2016): 137-152. https://doi.org/10.1016/j.jnca.2016.01.008

[12] Majlis Keselamatan Negara. Malaysian Cyber Security Strategy (MCSS) 2020 – 2024, National Cyber Security Agency (NACSA), Malaysian National Security Council. 2020.

[13] Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), National Cyber Security Agency (NACSA), Malaysian National Security Council. 2016.

[14] Herrera Montano, Isabel, José Javier García Aranda, Juan Ramos Diaz, Sergio Molina Cardín, Isabel De la Torre Díez, and Joel JPC Rodrigues. "Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat." *Cluster Computing* 25, no. 6 (2022): 4289-4302. https://doi.org/10.1007/s10586-022-03668-2

[15] Patz, Ronny. "Leaking, leak prevention, and decoupling in public administrations: the case of the European Commission." *West european politics* 41, no. 4 (2018): 1049-1071. Https://Doi.Org/10.1080/01402382.2017.1394103

[16] Hanafi, Hafizul Fahri, Mohd Helmy Abd Wahab, Abu Zarrin Selamat, Mohd Zahuri Khairani, Syed Zulkarnain Syed Idrus, and Muhamad Hariz Adnan. "Technology acceptance of a mobile augmented reality learning application among primary school students: A focus on the moderating effects of gender." In *AIP Conference Proceedings*, vol. 2608, no. 1. AIP Publishing, 2023. https://doi.org/10.1063/5.0127739