FOLDER VAULT IMPLEMENTATION ON AN INTANGIBLE-BASED E-COMMERCE

[1]ABDUL SYUKUR, [2]ARIS MARJUNI

[1,2]Faculty of Computer science, Dian Nuswantoro University, Semarang, Indonesia
E-mail: [1]abah.syukur01@gmail.com, [2]aris.marjuni@dsn.dinus.ac.id

Abstract- Digital goods are being popular in order to the growth of creative industries. As an industries based on individual creativity, almost creative industries product are formed as a digital or intangible products, such as music, digital design, photo and image, video, interactive games, software, script, and many more. Based on the creative industries value chain, there are creation, production, distribution, and commercialization process of digital creative products. There is not any difficulties for creative people to create and produce any creative products. However, the distribution and commercialization process often have some problems and barriers for creative industries. Regarding to their haracteristics, unauthorized party can modify, duplicate, or distribute the digital goods easily. In the commercialization context, these intellectual property infringements should be avoided by increasing the management of digital products inventory. In an intangible-based e-commerce, digital goods asset should be protected so that only authorized buyer or customer can download the products. It means that the download links and digital goods folder must be protected, namely folder vault. This paper discussed an implementation of folder vault to hide the original download link so that the downloadable files folder cannot be revealed to customer directly.

Keywords- Digital Goods, Intangible Products, E-Commerce, Folder Vault, Download Link.

I. INTRODUCTION

The rapid of technological developments provide a very positive impact in the creative industry. With the current technologies, the creative people can easily create, produce and distribute their creative products to be a creative economy values. Creative product does not provide any benefit unless those products converted into economic value. E-commerce is one of the most suitable media to support the commercialization of digital products into economic value. The creative peoples can sell their digital creative products through e-commerce, such as photos, graphic design, script, software, music, video, interactive games, and more. This e-commerce system can be developed in a variety of levels, either individually or portal websites.

Related to the intangible products which it's usually as a digital content form, creative industries need to consider the following content aspects (Rousseau, 2015), that are: (1) creating and protecting content; digital content provides an unique opportunity for innovation and creativity, but requires a method to protect it from theft and abuse. The presence of internet will also open a new opportunities for intellectual property infringement which can obstruct the innovation and creativity; (2) accessing and discovering content; there are a billion digital content in the world and it need a special attention to grab the potential users. So, it is very important to provide an access mechanisms and reliability of content search, such as design standards, metadata, and search engine optimization; (3) sharing and using content; digital content have an ability to be produced and distributed without cost and with minimal risk, and can be used repeatedly without becoming obsolete; (4) managing and preserving content; digital content opens up possibilities for grouping and stored in a larger volume, but it has the lost or damaged risk easily. Therefore, managing and preserving the digital content are needed for a sustainable use; (5) understanding and awareness of content; digital content has been changed the perception of information, knowledge, and material values. In the transition to the digital age, the understanding and concern for the environment of digital content is needed in order to make choices, decisions, and the right investment.

In order to digital goods market, there are many issues of selling intangible goods online (Bhattacharjee et al., 2011) which are: (1) digital goods risk management, (2) transformation of the technology-enabled value chain, (3) market impacts of legal decisions and legal agreements, and (4) transnational and cross-cultural issues. As an e-service, there are many measurements to evaluate a quality of an intangibility of e-commerce (Moon, 2013), which are: (1) information content, (2) reliability, (3) security, and (4) customization. Based on its characteristics, many different buyers can buy the same digital goods. After made a complete payment, then buyers will receive their ordered products directly.

This delivery can performed by download link through email or buyer's account. The link usually contains a path of product location, including folder, subfolder and file names. However, providing a full path to the buyer is certainly not a good way for security aspect. Because once buyers know the URL address, then they can download repeatedly as many times they want (Jin and Zbarsky, 2008). They might also explore another product in the same folder and

trying to download them without permission and bypassing the payment process. Hence, it is necessary to provide a folder or file vault so that unauthorized party cannot recognize the digital goods folder location or files. In this paper will present the use of vault methods to protect digital goods in an intangible e-commerce with and without an encryption algorithm to hide data folder such that only authorized buyer allows to access the download link.

II. DATA VAULT SYSTEM

Regarding to the data vault, a personal data vaults (PDVs) was proposed as a privacy architecture in which individuals retain ownership of their data (Moon et al., 2010). Before shared, data are filtered with content-service providers, and users or data custodian services. Online safe vault is developed that allows users to securely store their passwords online (Englert and Shah, 2009). Passwords are stored encrypted in the safe vault server and transmitted over the network as encrypted passwords.

The data vault is also proposed to facilitate science data analysis (Ivanova et al., 2013). Through the extension of the database system architecture, the scientific file repositories are opened transparently for efficient in database processing and exploration. Data are loaded from the repository without data ingestion. In order to digital goods marketplace, the digital vault for securing of digital goods repository is developed to protect and load a stored digital products.
In order to the security of digital content distribution, Fernandez (2005) explained an economic models of fair use to bridge the gap between traditional analog content and digitally protected content through digital right management.

III. PROPOSED METHOD AND DISCUSSION

Digital content is subject to discriminatory treatment rather than a tangible goods, it implies that digital goods should be protected from unauthorized buyers in term of sale of goods. There are many ways to protect the digital goods asset after uploaded to the web server. In this paper, we will discuss the use of cryptographic and non- cryptographic methods to hide the real download link, which will sent to customer or buyer.
In the common digital goods marketplace, after buyers made a complete payment then they will receive a download link of the paid products. Those methods will be implemented through the folder vault, which is suggested to hide, or protect a folder and files that are stored on the web server, as illustrated in Figure 1. By hiding the download link it will help the vault system to protect digital goods asset location, because unauthorized customers cannot see the real folder where the digital goods are stored through download link.

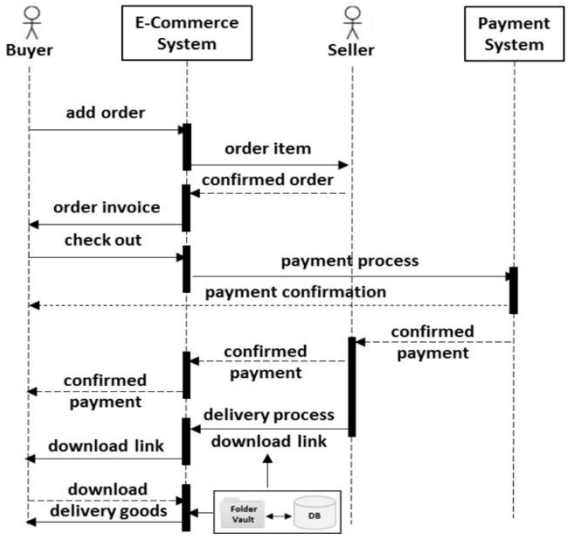

Fig. 1: Folder Vault Sequence Diagram

3.1. Hiding Link with Cryptographic Methods

The use of cryptographic method is very popular to increase secure download link, whether hashing or encryption algorithms. Suppose, customer buy a digital goods 'FileName.pdf' that stored in a folder, namely 'FolderName'. The related download link is http://YourSite.ext/FolderName/FileName.pdf".This method will mask the folder name using a hashing algorithms and/or encryption algorithms such that the encrypted download link will look like as http://YourSite.ext/EncryptedFoldeName/FileName.pdf. This encrypted download link can be provided through customer's email or e-commerce account, as shown in Figure 2 for an example.

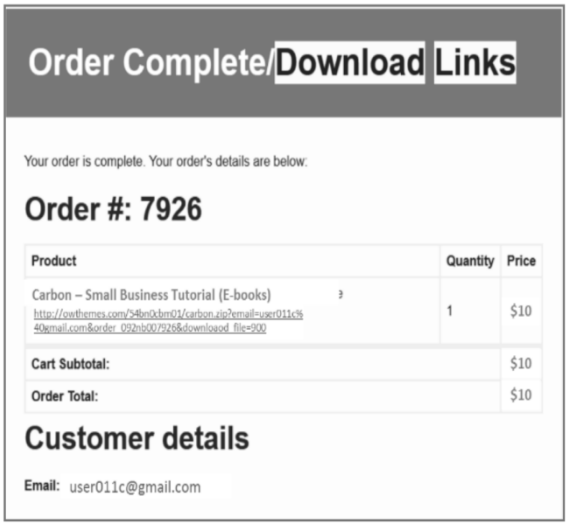

Fig. 2: Download Link Encryption Example

In this method, encrypting process may use any hashing algorithms, such as SHA1, SHA256, MD5, MD4, etc., and/or encryption algorithms, such as DES, AES, RSA, etc. For details, Figure 3 illustrate the hiding link scheme with the following steps:
(1) Identify the path or full path without or with domain name, which will encrypted.
(2) Generate hash values using hashes algorithms.

(3) Encrypt the hashes folder using encryption algorithms with a secret key.
(3) Reconstruct the new path as an encrypted download link.

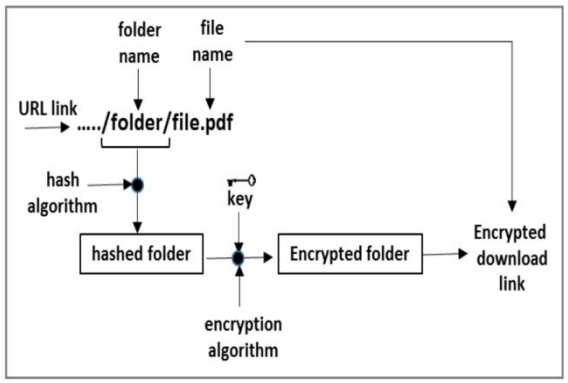

Fig. 3: Download Link Encryption Process

3.2. Hiding Link without Cryptographic Methods

Suppose, customer buy digital goods, namely "FileName.pdf" that is stored in a folder, namely 'FolderName' with the download link address is http://YourSite.ext/FolderName/FileName.pdf". To hide the file location, this method will change the real download link such that it will look like http://YourSite.ext/download.php?file=FileName.pdf. To make more secure, the folder location can be created outside the website document root so that it cannot serve the digital goods by direct link.

```
header("Pragma: public");
header("Expires: 0");
header("Cache-Control: must-
   revalidate, post-check=0,
   pre-check=0");
header("Cache-Control:
   public", false);
header("Content-Description:
   File Transfer");
header("Content-Type:
   ".$type);
header("Accept-Ranges:
   bytes");
header("Content-Disposition:
   attachment;
   file=\"".$HeaderFile.
   "\";");
header("Content-Transfer-
   Encoding: binary");
header("Content-Length:
   ".filesize($FileName));
```

Fig. 4: Header Setting

There are many implementation method to hide download link without using cryptography algorithm. For implementation example in PHP script, it can be performed by modify the HTTP headers as shown in Figure 4. Let, the root of website is "/YourSite" and the digital goods are stored in folder "/inventory/" located outside the website root.

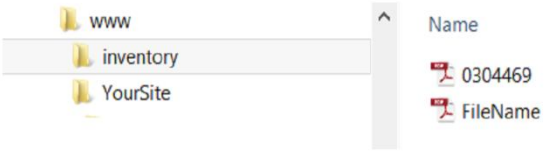

Fig. 5: Folder Structure

By Figure 5, the individual link for FileName.pdf is '/inventory/FileName.pdf. After modified headers, the downloadable files will be accessed from website root through download.php files with URL link http://YourSite.ext/download.php?file=FileName.pdf. Using this method, the real location of downloadable files are not revealed by customer and redirected to the website root. Although this method is not fully secure, at least the downloadable files are not accessed by direct links.

Fig. 6: Download Link Example

To ensure that only authorized buyer allow to download, then the download link can be combined with some parameters, such as buyer id, order id and product id, so the download link will look like http://YourSite.ext/download.php?id=buyer_id&file=file_id&order=order_id, such as illustrated in Figure 7 below.

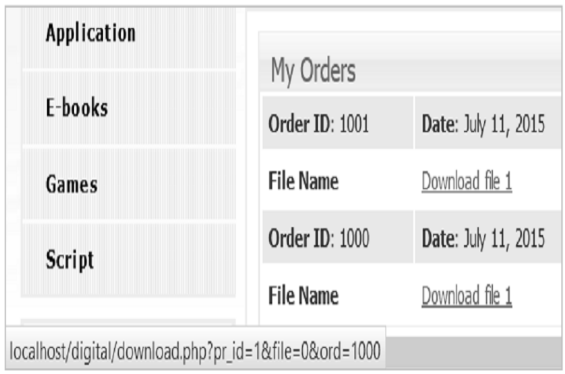

Fig. 7: Download Link with Some References Example

Another method to hide the folder of digital goods files is to use a temporary folder, as illustrated in Figure 8, with the following basic steps:
(1) Create a temporary folder. This directory can be created randomly using random number generator function. The use of random directory aims to create a limited access for customer. It means that one downloadable file only be accessed by one customer and customer cannot access another files.
(2) Copy the digital goods file to the temporary folder: The ordered products that selected by customer will be copied into the temporary folder so that customer cannot identify another products except their ordered items.
(3) Provide download link to customer to download the ordered digital goods in the temporary folder. No need to modify the download link in this step because the download link is redirected to the temporary folder.
(4) Delete temporary folder (if needed). If the system has a rule that customer only allowed to download ordered items in a limited number, then the temporary folder will be deleted automatically by system.

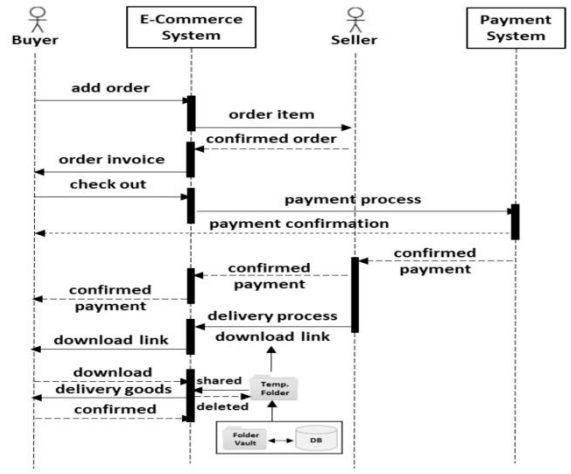

Fig. 8: Download Link with Temporary Folder

CONCLUSIONS

Hiding the download link that is provided for customer in the digital goods market or intangible-based e-commerce has been presented in this paper with the folder vault as the proposed method. The implementation of folder vault to protect the digital goods in the inventory database through hiding the download link is expected to provide some benefits, among others, to avoid unauthorized party to download the digital goods directly so that preventing theft of digital goods asset.

ACKNOWLEDGMENTS

This work was supported by the Directorate General of Higher Education, Ministry of National Education, Republic of Indonesia, under the Competitive Grant Research, 2015.

REFERENCES

[1]. S. Bhattacharjee, R. D. Gopal, J. R. Marsden, and R. Sankaranarayanan, “Digital goods and markets: emerging issues and challenges”, J. of ACM Transaction on Management Information System, vol. 2, no. 2, pp. 8-14, 2011.
[2]. Y. J. Moon, “The tangibility and intangibility of e-service quality”, Int. J. of Smart Home, vol.7, no.5, pp. 91-102, 2013.
[3]. H. Jin, and V. Zbarsky, “Enabling secure digital marketplace”, in Proc. of the 17th Int. World Wide Web Conference, pp. 1217-1218, 2008.
[4]. M. Mun, S. Hao, N. Mishra, K. Shilton, J. Burke, D. Estrin, M. Hansen, and R. Govindan, “Personal data vault: a locus of control for personal data streams”, in Proc. of the 6th Int. Conf. Co-NEXT '10, pp. 17:1-17:12, 2010.
[5]. B. Englert, and P. Shah, “On the design and implementation of a secure online password vault”, in Proc. of Int. Conf. on Convergence and Hybrid Information Technology (ICHIT 2009), pp. 375-382, 2009.
[6]. M. Ivanova, M. L. Kersten, S. Manegold and Y. Kargın, “Data vaults: a database welcome to scientific file repositories”, Journal Computing in Science and Engineering, vol. 15, no. 3, pp. 32-42, 2013.
[7]. B. Fernandez, “Digital content protection and fair use: what's the use?” Journal on Telecomm. High Technology, vol. 3, pp. 425-452, 2005.
[8]. A. Marsoof, “Digital content and the definition dilemma under the Sale of Goods Act 1979: Will the Consumer Rights Bill 2013 remedy the malady”, J. Int. of Commercial Law and Technology, vol. 9, no.4, pp. 285-293, 2014.
[9]. R. Rousseau, “Getting cozy with your content”, http://blog.optimityadvisors.com/?p=1031.

★★★