Monitoring System with Two Central Facilities Protocol
Caesar Firdaus, Wahyudin, and Eddy Prasetyo Nugroho*

Program Studi Ilmu Komputer, Departemen Pendidikan Ilmu Komputer, Universitas Pendidikan Indonesia, Jl. Dr. Setiabudhi No. 229 Bandung 40154, Indonesia

*Correspondence: email: eddypn@upi.edu

A B S T R A C T S
The security of data and information on government’s information system required proper way of defending against threat. Security aspect can be achieved by using cryptography algorithm, applying information hiding concept, and implementing security protocol. In this research, two central facilities protocol was implemented on Research and Development Center of Mineral and Coal Technology’s Cooperation Contract Monitoring System by utilizing AES and whitespace manipulation algorithm. Adjustment on the protocol by creating several rule of validation ID’s generation and checking processes could fulfill two of four cryptography objectives, consist of authentication and non-repudiation. The solid collaboration between central legitimization agency (CLA), central tabulating facility (CTF), and client is the main idea in two central facilities protocol. The utilization of AES algorithm could defend the data on transmission from man in the middle attack scenario. On the other hand, whitespace manipulation algorithm provided data integrity aspect of the document that is uploaded to the system itself. Both of the algorithm fulfill confidentiality, data integrity, and authentication.

© 2017 Tim Pengembang Jurnal UPI

ARTICLE INFO
Article History:
Received 03 February 2017
Revised 07 February 2017
Accepted 12 February 2017
Available online 01 April 2017

Keyword:
Protokol, Two Central Facilities, AES, Whitespace Manipulation, Cryptography.

DOI: http://dx.doi.org/10.17509/ijost.v2i1
p- ISSN 2528-1410 e- ISSN 2527-8045
1. INTRODUCTION

Today, the use of information technology influences various fields, such as health, education, government, politics, and so on. (Hurd, 1998) Security aspect must be taken seriously by considering variety of both general and confidential information exchanged through the network. (Cheminod et al., 2013) Both personal and government data do not immune to the threat from irresponsible parties. (Sartor, 2013) Security measure to this particular problem can be achieved using cryptography and information hiding in order to improve the security aspect of the information and communication technology (ICT) based system. (Liao & Hsiao, 2014)

The main security problems in e-government are confidentiality, information integrity, authentication toward information or copyright protection, non-repudiation, and more. (Lambrinoudakis et al., 2003) ICT based system’s security has to provide protection toward the secrecy of the data itself. Security, authentication, and verification must be applied in line with privacy, and the government must ensure on securing the confidentiality of the information. Basically, digital watermarking is a tool to keep the copyright or to authenticate copyright of digital data. However, its mature digital watermarking can improve the security of e-government system (Sharma et al., 2007). For example, mineral and coal research and development center’s cooperation contract monitoring system is a system developed to monitor cooperation contract data. This system has the ability to attach files to particular cooperation contract data. Affiliation staff can upload PDF files of a scanned contract. (Sun et al., 1994) This example was applied and confirmed that reported contract data with its attachment is required to be secured due to its high value of information.

In this particular research, the cooperation contract monitoring system will be modified by using two central facilities protocol and implementing both Advanced Encryption Standard (AES) and whitespace manipulation. The protocol will authenticate the user. Thus, this can maintain that only authenticated user has access to the system. Whitespace manipulation algorithm will be used to claim the PDF files so it can keep the data integrity. On the other hand, AES algorithm provide the ability to encrypt and decrypt data on transmit. This research will give a new view of the two central facilities protocol’s utilization outside of e-voting sector.

2. LITERATURE REVIEW

2.1. Cryptography

Cryptography is derived from Greek, cryptos that mean secret and graphien which mean writing. Cryptography can be interpreted as secret writing. Cryptography is science and art to keep secret message. (Diffie & Hellman, 1976) Cryptography is a study of mathematical technique that related with information security aspect such as confidentiality, data integrity, authentication, and non-repudiation. (Siponen & Oinas-Kukkonen, 2007) Cryptography has four main objectives:

(i) Confidentiality. Cryptography used to keep the message from irresponsible parties that have no right to access the message or information. Confidentiality can be achieved by using physical or mathematical algorithm security measure.

(ii) Data Integrity. In order to keep data integrity, system need to have the ability to detect any change on the data by irresponsible parties that have no right to make any change. The data...
manipulations consist of insertion, deletion, and substitution.

(iii) Authentication. Authentication is a function that is highly related with identification. The parties that are communicating in a system should be identified one to another. Authentication does not only applied to the communicating parties but also the information that preserve its authenticity.

(iv) Non-repudiation. Non-repudiation is a function to prevent any denial to an act or event that actually happen. For example, a party could not admit if received some funds if there is a receipt that mentioned the amount of its transaction with both name and sign of the sender.

3.2. ADVANCED ENCRYPTION STANDARD (AES)

Advanced Encryption Standard (AES) is cryptography algorithm that designed to operate with 128 bit block message and used three variation of key with 128, 192, or 256 bit. In 2001, AES was used as the new standard of cryptography algorithm which is published by National Institute of Standard and Technology (NIST) as the successor of Data Encryption Standard (DES). (Thakur & Kumar, 2011) AES is a cryptography algorithm that operate with 128 bit block message and has three variation of key. Specific key size will determine the number of iteration in this algorithm. (Potlapally et al., 2006) The characteristic of each AES algorithm showed in Table 1. The outline of AES algorithm showed in Figure 1. In general, four main processes in AES algorithm consist of:

a. SubBytes (Byte Substitution Transformation).

b. ShiftRow (Byte Shifting Transformation).

c. MixColumns (Column Mixing Transformation).

d. AddRoundKey (Add Key Transformation).

2.3. INFORMATION HIDING

Information hiding is a form of secret communication while transmitting information. Information hiding is a measure to embed the ownership information and distribution destination detail of a picture or music digital content. Steganography is an information hiding with communication purpose. On the other hand, digital watermarking is used to preserve the intellectual property right. (Al-Othmani, 2009)

Figure 2 shows the classification of information hiding based on the used technique. Watermarking emphasizes the copyright marking, which is used to claim the ownership of a copyright, while steganography emphasizes on the form of secret communication. (Petitcolas, 1999)

<table>
<thead>
<tr>
<th>Key Size (Nk words)</th>
<th>Block Size (Nb words)</th>
<th>Iteration (Nr)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-128</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>AES-192</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>AES-256</td>
<td>8</td>
<td>14</td>
</tr>
</tbody>
</table>

Table 1. AES version conditions
2.4. WHITESPACE MANIPULATION

Information hiding on digital document can be achieved by manipulating some components within the document. The manipulation can be categorized as toline shift coding, word shift coding, whitespace manipulation, and text content. (Sullivan et al., 2010) Whitespace means space and tab in a text document. When giving the right data, this approach the manipulation can keep some data. The rule of embedding data can be manipulated according to the developer. (Por et al., 2008)

2.5. TWO CENTRAL FACILITIES PROTOCOL

Two central facilities protocol is a protocol, which is developed to handle voting using two central facilities, Central Legitimization Agency (CLA) and Central Tabulating Facilities (CTF). CLA is a facility which is responsible to verify the user by using series of process, while CTF is facility to tabulate all data. (Muharram & Satrya,
Two central facilities for voting purposes are (See Figure 3)

a. Every voter sends message to CLA and request validation number.

b. CLA send random validation number. CLA save a list of validation number with. CLA save a list of validation number receiver.

c. CLA send list of validation number to CTF for validation need.

d. Every voter chooses an identity number. The message will be send with the identity number to CTF alongside with the validation number.

e. CTF check and compare the validation number from voter and validation number from CLA.

f. CTF shows the result of voting.

---

**Figure 2. Information hiding classification**

**Figure 3. Voting with two central facilities**
3. METHODS

The present study involved five steps, in which these steps are described in the following (See Figure 4):

(i) Literature Review.

Cryptography and Network Security Principle provided the quiresence of network security and AES algorithm which acts as an important role in security factors. This provided a solid knowledge forming understanding towards network security. The rest of the journals also provide the supplemental material that gave additional insight in this research

(ii) Cooperation contract monitoring system modification.

In this step, modification of cooperation contract monitoring system has been done by implementing previous concepted two central facilities protocol, AES, Information Hiding, and Whitespace Manipulation. Two central facilities protocol will allow system to filter or to determine the user by its previledge. Whitespace manipulation is used to insert certain information that act as verifier to keep its integrity. AES was used when transmitting data. The result from this step is the modified cooperation contract monitoring system.

(iii) Software development

Software development was done using sequential linear method, which consists of analystist, design, coding, and testing.

(iv) Theory testing.

(v) Final stage documentation

4. RESULTS AND DISCUSSION

4.1. Monitoring System with Two Central Facilities Protocol

We developed two central facilities protocol by dividing into three different sub systems, voter client, CLA, dan CTF. This protocol is developed to ensure security and minimize the load of each sub system. Both CLA and CTF have different database with different organizations according to each function. There are several modifications to this protocol in order to implement it to cooperation contract monitoring system. These are the conducted modification (See Figures 4-6):

1. CLA authenticates user by username and password given.
2. CLA sends validation ID to user in every session.
3. Every user has more than one validation ID. Validation ID was generated every time the user attempt to login into the system.
4. CLA and CTF save generated validation ID with specified staff ID.
5. CTF identifies user’s validation ID before executing every major function in the system.
4.2. User Authentication

User will be given random 16 digits of validation number after CLA authenticate the username and password. Validation ID is used by CLA and CTF to determine whether the user has access or not to access the system. This research uses 16 digits of numeric validation ID, for example “2222578348197275”. After generated, validation ID will be stored in CLA and CTF in chipertext form by using AES algorithm. Validation ID is used in two step authentication.

In the developed system, client will trigger two step authentication that performed by CLA and CTF. Both CLA and CTF will check the validation ID in current session with the stored validation ID in both databases. By doing so, system could prevent any unauthorized user.

Table 2 shows the general description of monitoring system with two central facilities.
protocol. There are three main components that communicate with one to another.

![Monitoring System with Two Central Facilities Protocol Architecture](image)

**Figure 5.** Monitoring system with two central facilities protocol architecture

<table>
<thead>
<tr>
<th>Component</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Interacting with user. Showing received data from CTF.</td>
</tr>
<tr>
<td>CLA - Central Legitimization Agency</td>
<td>Authenticate user.</td>
</tr>
<tr>
<td>CTF - Central Tabulating Facility</td>
<td>Serving contract data request, storing file uploaded by user.</td>
</tr>
</tbody>
</table>

### 4.3. AES 128 bit Implementation

AES-128 is chosen as the cryptography algorithm to securing data on transmit between every sub system by considering the performance of the system. In every iteration there are several mathematical transformations applied to the data. The transformations consist of SubBytes, ShiftRows, MixColumns, dan AddRoundKey.

Chipertext is the result of the mathematical transformation. AES-128 uses symmetric key while encrypting and decrypting. Here is an example of encryption result using AES-128 is shown in Table 3.

In the xml files, every field is in chipertext form. The destination will decrypt this file then process it according to specified function. This kind of transmission occurred between client to server, and server to server.
4.4. Watermark Insertion using Whitespace Manipulation

The uploaded PDF files is processed in order to keep the security while the data is on transmission. The system can verify the uploaded PDF files using whitespace manipulation algorithm. PDF file as cover media will be inserted with a text using whitespace manipulation. This will ensure the data integrity of PDF file (See Figures 6-8).

Watermark is inserted after “%EOF” tag. This tag marked the end of file. This position is choses by considering the suspiciousness of ther party. The inserted watermark will be showed as a plain space or null. The process is showed in the Figures 9 and 10. The spaces in Figure 10 showed the inserted watermark. The insertion process takes 0.0316 second.

Both database keep the data in chipertext form. By avoiding unnecessary encryption and decryption, the time and load needed will be decreased. An example of data transmitted between CTF and client are shown in Figures 7 and 8.
Tabel 3. Encryption Result using AES-128

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Chipertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>PT. Inti Bangun Sejahtera Tbk</td>
<td>70 d9 f9 d5 45 51 6e 22 61 78 27 3c aa 61 d0 ad ca 24 6c 33 0a cb 7f c3 3f 5c 59 b2 81 c0 06 71</td>
</tr>
</tbody>
</table>

<?xml version="1.0" encoding="utf-8"?>
<xml>
<substansi>7e7231c8c6fd61fc5654e1dd56237415386a8e0e7edaa408e8d1ef4b57084fcdfb511f8b98bb02182c5890a7f9f87187730b41bcb333359cf2f69c1de669609b117760e968324186b326a507f7c3cb06b705d9101611173674d442d73d40caaf937e1904556c77de1d3f0c2a6b</substansi>
<nomor>781241571cccb28459a191ee5635e857d9f448fcec5c31ac2edd17b8e05e5422b</nomor>
<jenis_kontrak>5acb28a402480930cc22b8d34a3a0b6e</jenis_kontrak>
<tgl_berakhir>7b4f1650278bd1347739e06243c50e33</tgl_berakhir>
<tgl_mulai>babdc9669a50c557faa157036dfe8fa7</tgl_mulai>
<availability>042870b4bdf008718c54e5a02355f40</availability>
<nilai>87bc633a0cf4a26f304c99eaf1c056d0</nilai>
<timestamp>8492ec4d1dc9a873d03a998260370a543d45ef6de7e9d62de248db5758099bd</timestamp>
<id_alamat>042870b4bdf008718c54e5a02355f40</id_alamat>
<nama>3753a1f75c6d615eb0786e5c59f2099109c0dc534e506753f86d038e17bf91ef</nama>
<jenis_mitra>042870b4bdf008718c54e5a02355f40</jenis_mitra>
</xml>

Figure 7. Data on transmit between CTF

DOI: http://dx.doi.org/10.17509/ijost.v2i1
p-ISSN 2528-1410 e-ISSN 2527-8045
4.4. Implementation

In this part, the result of implementation will be showed. The flow of authentication can be described as:

a. User input username and password on login page.
b. Client receive user’s input then encrypt it.
c. Encrypted username and password are sent to CLA
d. CLA receive username and password.
e. CLA decrypt username and password and check it with the data stored in database.
f. CLA check the username and password.
g. When the username and password match, CLA will generate validation ID.
h. CLA encrypt validation ID with CLA key.
i. CLA store validation ID to database.
j. Encrypted validation ID stored in browser’s session.
k. CLA encrypt validation ID with CTF key.
l. CLA send encrypted validation ID to CTF.
m. CTF receive encrypted validation ID from CLA.
n. CTF store validation ID to its database.
o. CLA send request to client to show the data in dashboard page.
q. CLA and CTF melakukan check current session validation ID.

Validation ID matching is done by comparing current session validation ID to CLA and CTF stored validation ID. Validation ID matching example is stored in Figure 11. Validation ID matching is done by involving CLA and CTF so it can ensure the security and the system could not be deceived.

Figure 9. Insertion result using whitespace manipulation
5. TESTING

5.1. Man in the Middle Attack Scenario

Man in the Middle Attack Scenario is a testing scenario evaluating security aspect by eavesdropping data on transmission between two parties. This research will test sniffing attack form. Sniffing is a kind of attack that the attacker takes every single data packet on transmission.

By using wireshark, packet data on transmission between every sub system can be monitored. Figure 11 is the result of captured data packet between CTF and client. The data is on chipertext form or encrypted form. Sniffing attack type is useless against the scenario that included authentication using encryption. (De Vivo et al., 1998)

![Figure 11. Capture result using wireshark](image-url)
5.2. Turn Around Time

Turn Around Time is the total time needed of a plaintext to be encrypted and back to its original form (plaintext). This testing is done with 25 PDF files with 14 KB to 1.003 KB file size. The result of this testing is shown in Table 4.

Data from Table 4 are the tested files which obtained from PUSLITBANG tekMIRA and other journal from various website. Every pdf files consist of text, table, and figure. File size increased by 3.785 to 4.095 times. It occurred because PDF files was converted to hexadecimal resulted twice increased file size from the original. Every single string then encrypted with AES resulting chipertext with about two times length from the hexadecimal. On this point, the file size increased four times from the original.

5.3. Two Central Facilities Protocol Implementation Analysis

<table>
<thead>
<tr>
<th>No</th>
<th>File Name</th>
<th>File Size (in KB)</th>
<th>Time (in second)</th>
<th>Encrypt</th>
<th>Decrypt</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Daftar_KS_Kelitbangan_tekmira_2012-2013.PDF</td>
<td>14</td>
<td>2.173</td>
<td>8.008</td>
<td>10.181</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Kerjasama_LN_2006-2010.PDF</td>
<td>16</td>
<td>2.118</td>
<td>9.239</td>
<td>11.357</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>D2L_Learning_Repository_Brochure.PDF</td>
<td>52</td>
<td>7.532</td>
<td>32.553</td>
<td>40.085</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>chen5.PDF</td>
<td>84</td>
<td>12.363</td>
<td>65.913</td>
<td>78.276</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>mathjournal94.PDF</td>
<td>92</td>
<td>12.891</td>
<td>58.344</td>
<td>71.235</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Rencana_PT_Smelting_14_April.PDF</td>
<td>131</td>
<td>21.992</td>
<td>79.884</td>
<td>101.876</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Kontrak_Inti_2013.PDF</td>
<td>132</td>
<td>20.973</td>
<td>81.788</td>
<td>102.761</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Daftar_KS_tekmira_Korea_ongoing_2010-2012.PDF</td>
<td>171</td>
<td>23.401</td>
<td>108.33</td>
<td>131.761</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Perjanjian_Kerjasama_Kemitraan_Litbang_2006-2014.PDF</td>
<td>176</td>
<td>26.443</td>
<td>115.655</td>
<td>142.098</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Daftar_KS_tekmira_2010-2012.PDF</td>
<td>219</td>
<td>30.323</td>
<td>142.922</td>
<td>173.245</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>automatic_format_identification.PDF</td>
<td>250</td>
<td>37.243</td>
<td>173.657</td>
<td>210.900</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Daftar_KS_tekmira_Jepang.PDF</td>
<td>292</td>
<td>46.431</td>
<td>183.736</td>
<td>230.167</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>SecureOnlineVoting.PDF</td>
<td>297</td>
<td>44.842</td>
<td>206.178</td>
<td>250.66</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Analysis of LSB based Image Steganography Techniques.PDF</td>
<td>325</td>
<td>49.011</td>
<td>209.225</td>
<td>258.236</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>fmipa2012016.PDF</td>
<td>374</td>
<td>57.601</td>
<td>267.616</td>
<td>325.217</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Schneier.PDF</td>
<td>402</td>
<td>61.005</td>
<td>255.226</td>
<td>316.231</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Kontrak_Pelayanan_Jasa_2006-2014.PDF</td>
<td>413</td>
<td>58.057</td>
<td>263.158</td>
<td>321.215</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Draft_PT_Smelting_15_April.PDF</td>
<td>432</td>
<td>62.423</td>
<td>274.466</td>
<td>336.889</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>DK21713717.PDF</td>
<td>508</td>
<td>76.699</td>
<td>325.088</td>
<td>401.787</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>dct.PDF</td>
<td>595</td>
<td>88.962</td>
<td>385.769</td>
<td>474.731</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Chapter II.PDF</td>
<td>702</td>
<td>104.508</td>
<td>462.911</td>
<td>567.419</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>271332100014.PDF</td>
<td>755</td>
<td>109.941</td>
<td>483.805</td>
<td>593.746</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>spread_spectrum_image_steganography.PDF</td>
<td>906</td>
<td>132.747</td>
<td>577.424</td>
<td>710.171</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Universal Algorithm.PDF</td>
<td>1003</td>
<td>142.988</td>
<td>633.531</td>
<td>776.519</td>
<td></td>
</tr>
</tbody>
</table>
These are the effect of two central facilities protocol implementation on monitoring system. In short, the effect can be explained into two parameters. Discussion about this effect can be described in the following:

a. Comparison of single and two central facilities protocol

According to Darya Kurilova on Internet Security Protocols, there are some aspects that can be compared between security protocols. The comparison between single and two central facilities protocol is shown in Table 5.

b. Only authorized user authenticated.

By utilizing the communication ability between client CLA, and CTF, every single sub system helps each other to determine whether a user is authorized or not. It can be achieved by matching validation ID stored on both CLA and CTF.

5.4. Implication of Using Algorithm AES in Monitoring System on Two Central Facilities Protocol

These are the implication of algorithm AES in monitoring system using two central facilities protocol. In short, the impact can be classified into four topics, including confidentiality, data integrity, authentication, and non-repudiation. Discussion about this implication can be described in the following:

a. Confidentiality

Encryption and decryption process to data on transmit is a measure to provide confidentiality from unauthorized parties. Key that is used in this process consist of 16 digits of alpha numeric combination. A web owned by Foundstone said that it need 56 million years to brute force a 16 digits lowercase alpha numeric key with 4670K k/s calculation.

b. Data Integrity

AES algorithm is an algorithm that use symmetry key. It means, in order to encrypt or decrypt AES algorithm need the same exact key. The data integrity will be provided as long as the key remain secret.

c. Authentication.

Authentication to registrated user is done by using validation ID stored on both CLA and CTF database. A result of authentication testing is shown in detail in Table 6.

d. Non-repudiation

Authorized users have access to the system. The system will record every action that this type of user did while logging in.

5.5. Whitespace Manipulation Implementation Analysis

Whitespace manipulation algorithm could ensure data integrity from PDF file which uploaded to the monitoring system. It can be achieved by doing verification to the uploaded data. System’s log also showed that the verification involved both CLA and CTF.
6. CONCLUSION

By implementing two central facilities protocol in monitoring system, authentication and non-repudiation aspect can be fulfilled. With the predefined addition rule on this protocol, it could authenticate users that have the right to access the system, while the non-repudiation aspect fulfilled by logging system activity within the system. Both CLA and CTF can communicate to authenticate as a user. It is important to redefine the rule between CLA, CTF, and client in order to authenticate and responding to received request. The rule of generating and storing validation ID is also important things to watch.

AES and whitespace manipulation algorithm in monitoring system using two central facilities fulfill three of four main objectives of cryptography. It consists of confidentiality, data integrity, and authentication. AES algorithm could keep confidentiality of a data on transmit by processing it to encrypted form. Watermark embedding using whitespace manipulation to a PDF file could keep its data integrity and authentication. Embedding process is done on client side before client send the PDF file to CTF. The embedded watermark can be used to claim the ownership of data. It is important to keep the secrecy of AES key. By doing so, the data integrity will be provided as long as the key remain secret, while the embedding process using whitespace.
algorithm has to keep the PDF to be intact or uncorrupt.

7. ACKNOWLEDGEMENTS
Authors acknowledged Universitas Pendidikan Indonesia Jl. Dr. Setiabudhi No. 229 Bandung 40154 Jawa Barat – Indonesia for providing facilities for conducting the research activities.

8. AUTHORS’ NOTE
The author(s) declare(s) that there is no conflict of interest regarding the publication of this article. Authors confirmed that the data and the paper are free of plagiarism.

9. REFERENCES


DOI: [http://dx.doi.org/10.17509/ijost.v2i1](http://dx.doi.org/10.17509/ijost.v2i1)
P-ISSN 2528-1410 e-ISSN 2527-8045