Indonesian Journal of Science & Technology

Journal homepage: http://ejournal.upi.edu/index.php/ijost/

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

ABSTRACT

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.

ARTICLE INFO

Article History:
Submitted/Received 03 Dec 2016
First revised 07 Jan 2017
Accepted 27 Mar 2017
First available online 01 April 2017
Publication date 01 April 2017

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

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 cryptograhy 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

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

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. It 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 Sfhiting 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)

Tabel 1. AES version conditions

	Key Size (Nk words)	Block Size (Nb words)	Iteration (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

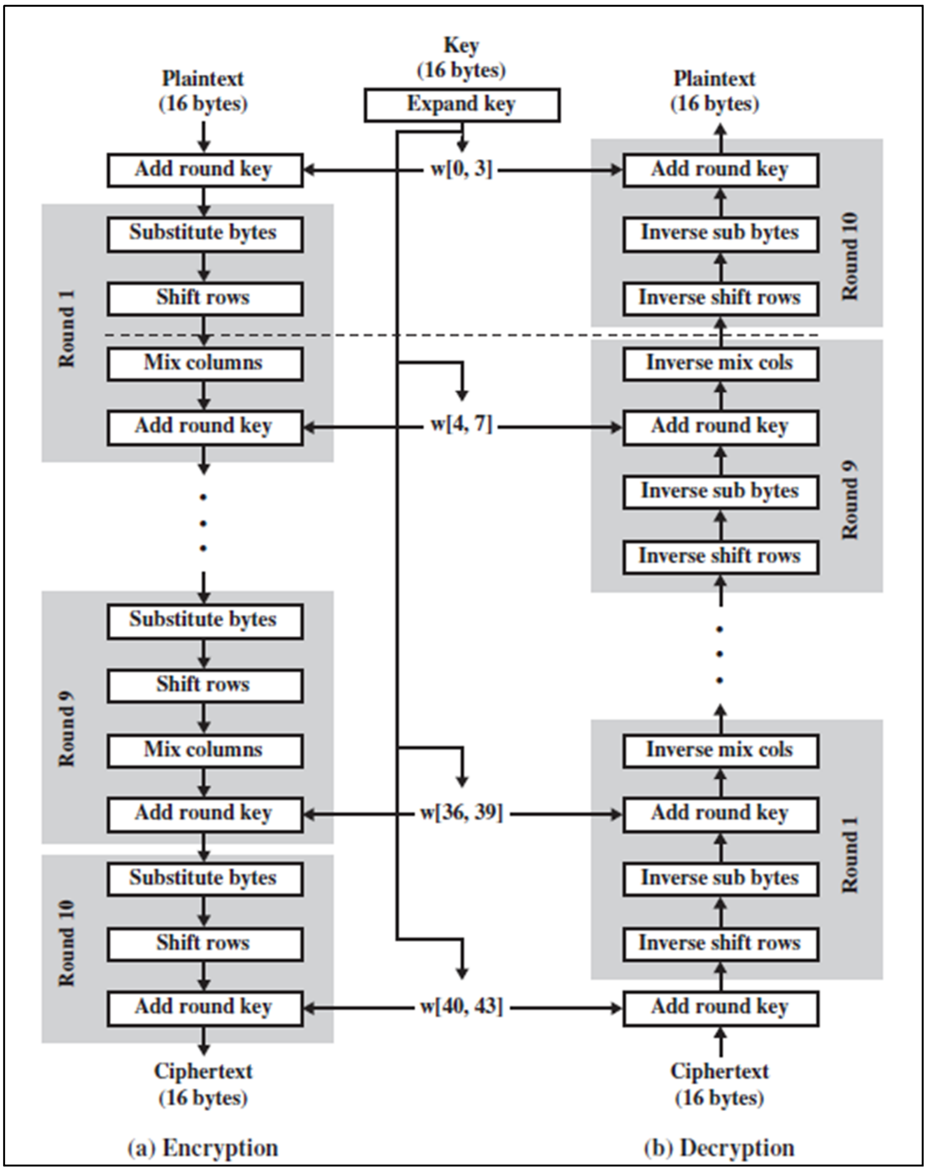


Figure 1. Encryption – decryption flow in AES algorithm

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 alldata. (Muharram & Satrya,

2016) 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 and validation number from CLA.
f. CTF shows the result of voting.

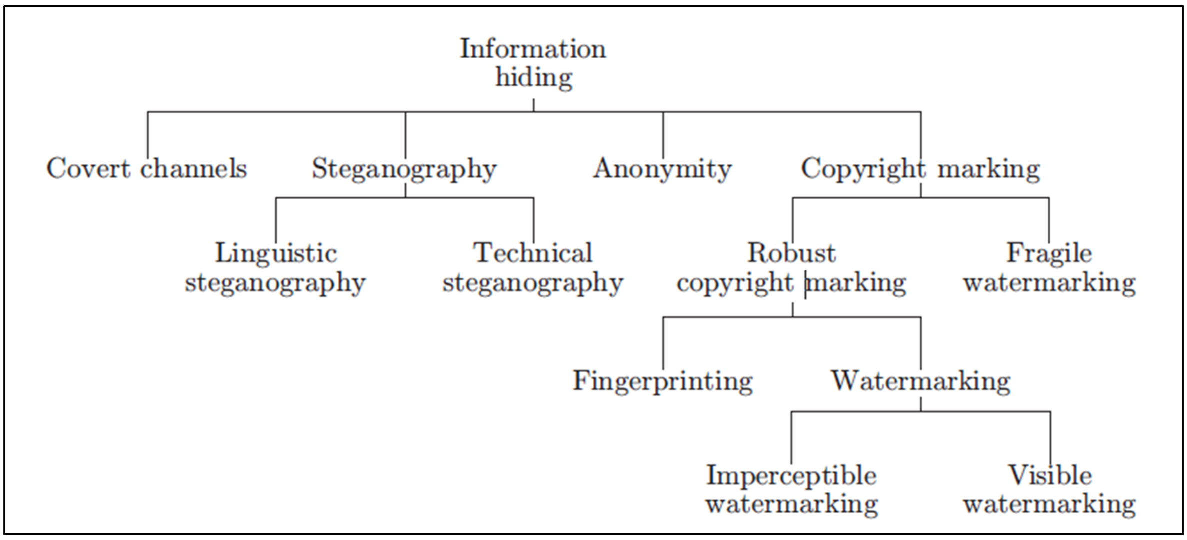


Figure 2. Information hiding classification

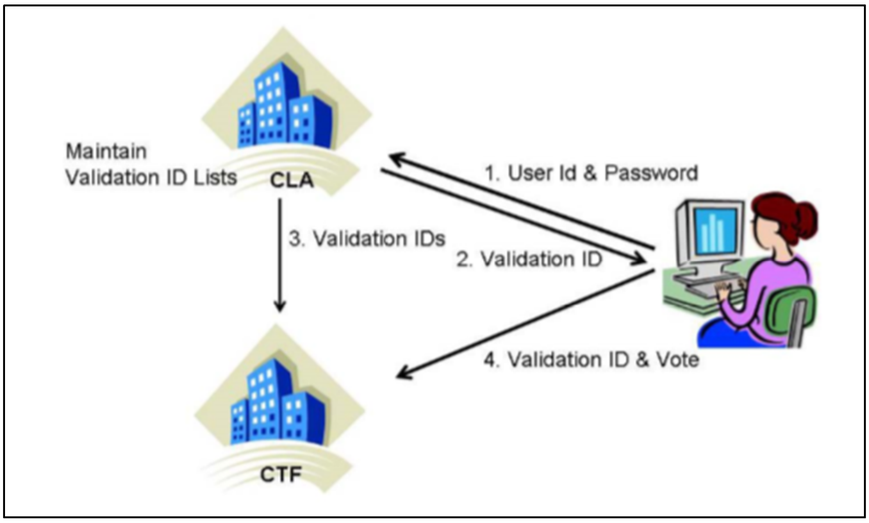


Figure 3. Voting with two central facilities

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

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 quitessence 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 analysist, 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.

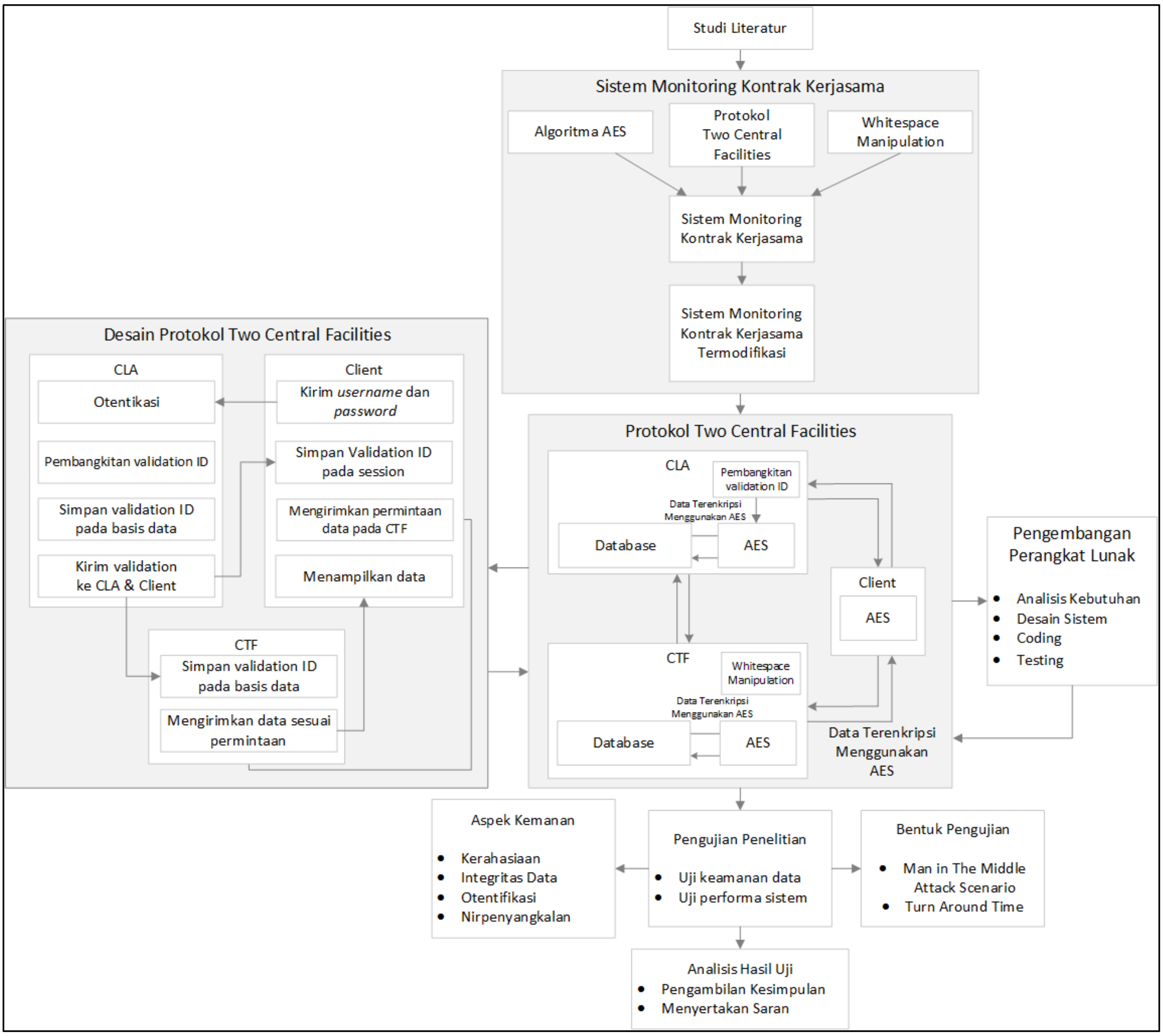

Studi Literatur
Sistem Monitoring Kontrak Kerjasama
Algoritma AES
Protokol Two Central Facilities
Whitespace Manipulation
Sistem Monitoring Kontrak Kerjasama
Sistem Monitoring Kontrak Kerjasama Termodifikasi
Desain Protokol Two Central Facilities
CLA
Otentikasi
Pembangkitan validation ID
Simpan validation ID pada basis data
Kirim validation ke CLA & Client
Client
Kirim username dan password
Simpan Validation ID pada session
Mengirimkan permintaan data pada CTF
Menampilkan data
CTF
Simpan validation ID pada basis data
Mengirimkan data sesuai permintaan
Protokol Two Central Facilities
CLA
Pembangkitan validation ID
Data Terenkripsi Menggunakan AES
Database
AES
Client
AES
CTF
Whitespace Manipulation
Data Terenkripsi Menggunakan AES
Database
AES
Data Terenkripsi Menggunakan AES
Pengembangan Perangkat Lunak
Analisis Kebutuhan
Desain Sistem
Coding
Testing
Aspek Kemanan
Kerahasiaan
Integritas Data
Otentifikasi
Nirpenyangkalan
Pengujian Penelitian
Uji keamanan data
Uji performa sistem
Bentuk Pengujian
Man in The Middle Attack Scenario
Turn Around Time
Analisis Hasil Uji
Pengambilan Kesimpulan
Menyertakan Saran

Figure 4. Research scheme

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 digitsof 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.

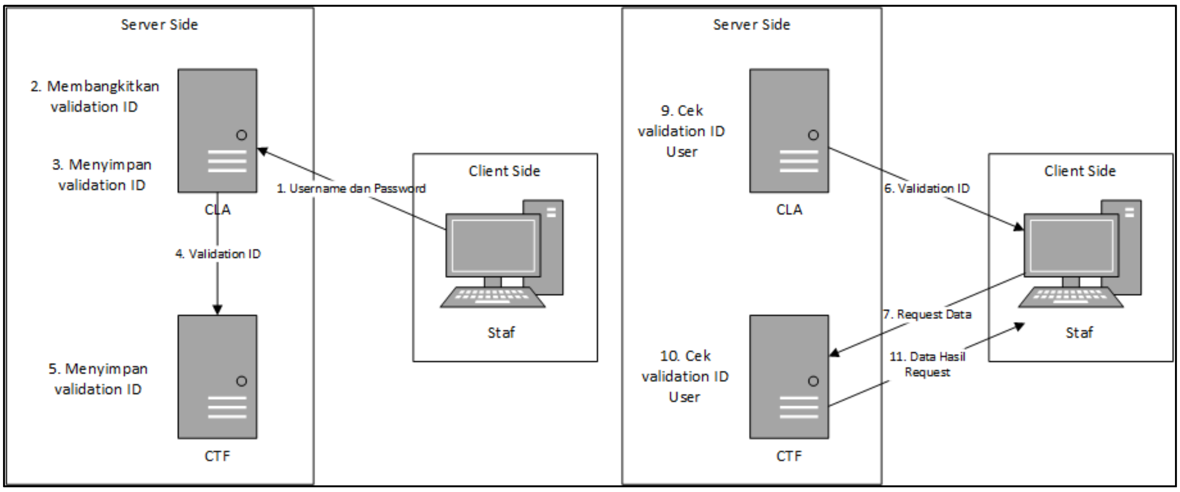


Figure 5. Monitoring system with two central facilities protocol architecture

Tabel 2. Monitoring system component

Component	Function
Client	Interacting with user. Showing received data from CTF.
CLA - Central Legitimization Agency	Authenticate user.
CTF - Central Tabulating Facility	Serving contract data request, storing file uploaded by user.

4.3. AES 128 bit Implementation

AES-128 is choosed 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 use symmetri 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.

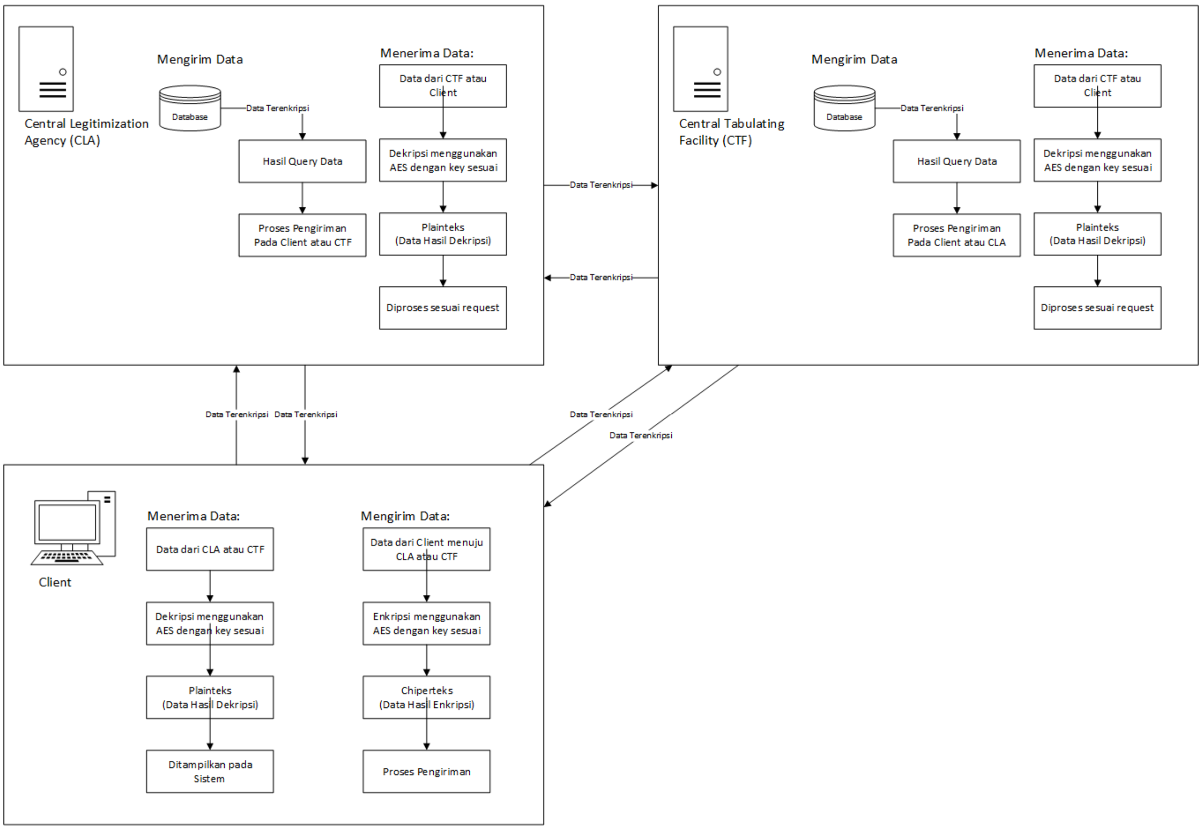

Central Legitimization Agency (CLA)
Mengirim Data
Database
Data Terenkripsi
Hasil Query Data
Proses Pengiriman Pada Client atau CTF
Menerima Data:
Data dari CTF atau Client
Dekripsi menggunakan AES dengan key sesuai
Plainteks (Data Hasil Dekripsi)
Diproses sesuai request
Data Terenkripsi
Data Terenkripsi
Central Tabulating Facility (CTF)
Mengirim Data
Database
Data Terenkripsi
Hasil Query Data
Proses Pengiriman Pada Client atau CLA
Menerima Data:
Data dari CTF atau Client
Dekripsi menggunakan AES dengan key sesuai
Plainteks (Data Hasil Dekripsi)
Diproses sesuai request
Data Terenkripsi
Data Terenkripsi
Data Terenkripsi
Data Terenkripsi
Client
Menerima Data:
Data dari CLA atau CTF
Dekripsi menggunakan AES dengan key sesuai
Plainteks (Data Hasil Dekripsi)
Ditampilkan pada Sistem
Mengirim Data:
Data dari Client menuju CLA atau CTF
Enkripsi menggunakan AES dengan key sesuai
Chiperteks (Data Hasil Enkripsi)
Proses Pengiriman

Figure 6. AES implementation in two central facilities protocol

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 chosed 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

Plaintext :	PT. Inti Bangun Sejahtera Tbk
Chipertext:	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

```
<?xml version="1.0" encoding="utf-8"?>
<xml>
<substansi>7e7231c8c6f6d1fc5654e1dd56237415386a8e0e7edaaa408e8d1ef4b57084fcdfb
511f8b98bb02182c5890a7f9f87187730b41bcb333359cf2f69c1de669609b117760e9683241
86b326a507f7c3cb06b705d9101611173674d442d73d40caafb937ce1904556c77de1d3fdc0c
2a86b</substansi>
<nomor>781241571ccb28459a191ee5635e857d9f448fcec5c31ac2edd17b8e05e5422b</no
mor>
<jenis_kontrak>5acb28a402480930cc22b8d34a3a0b6e</jenis_kontrak>
<tgl_berakhir>7b4f1650278bd1347739e06243c50e33</tgl_berakhir>
<tgl_mulai>babdc9669a50c557faa157036dfe8fa7</tgl_mulai>
<availability>042870b4bfdf008718c54e5a02355f40</availability>
<nilai>87bc633a0cf4a26f304c99eaf1c056d0</nilai>
<timestamp>8492ec4d1dc9a873d03a998263070a543d4d5ef6de7e9d62de248db5758099bd
</timestamp>
<id_alamat>042870b4bfdf008718c54e5a02355f40</id_alamat>
<nama>3753a1f75cbd615eb0786e5c59f2099109c0dc534e506753f86d038e17bf91ef</nama
>
<jenis_mitra>042870b4bfdf008718c54e5a02355f40</jenis_mitra>
<id>042870b4bfdf008718c54e5a02355f40</id>
</xml>
```

Figure 7. Data on transmit between CTF

.

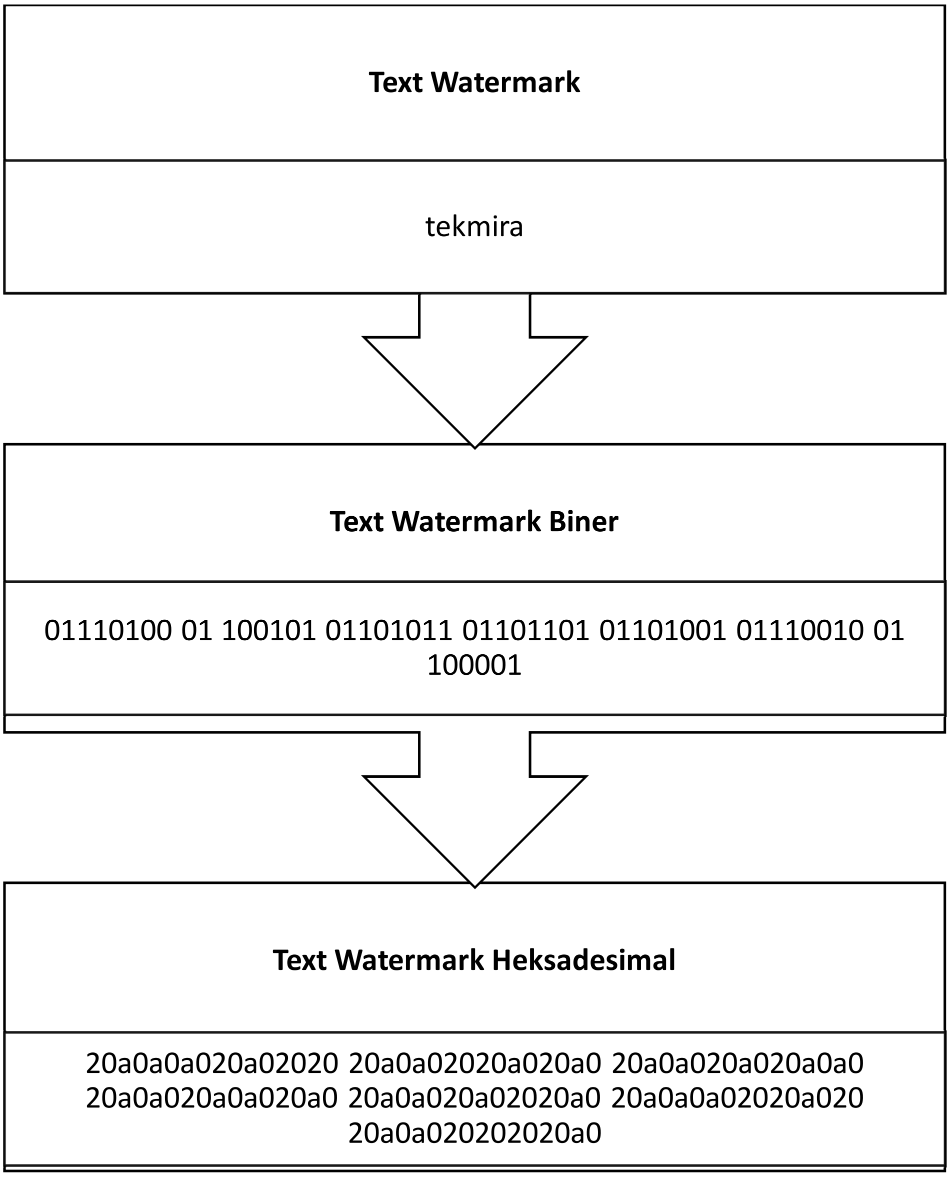

Text Watermark
tekmira
Text Watermark Biner
01110100 01 100101 01101011 01101101 01101001 01110010 01 100001
Text Watermark Heksadesimal
20a0a0a020a02020 20a0a02020a020a0 20a0a020a020a0a0 20a0a020a0a020a0 20a0a020a02020a0 20a0a0a02020a020 20a0a020202020a0

Figure 8. Text watermark transformation

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.

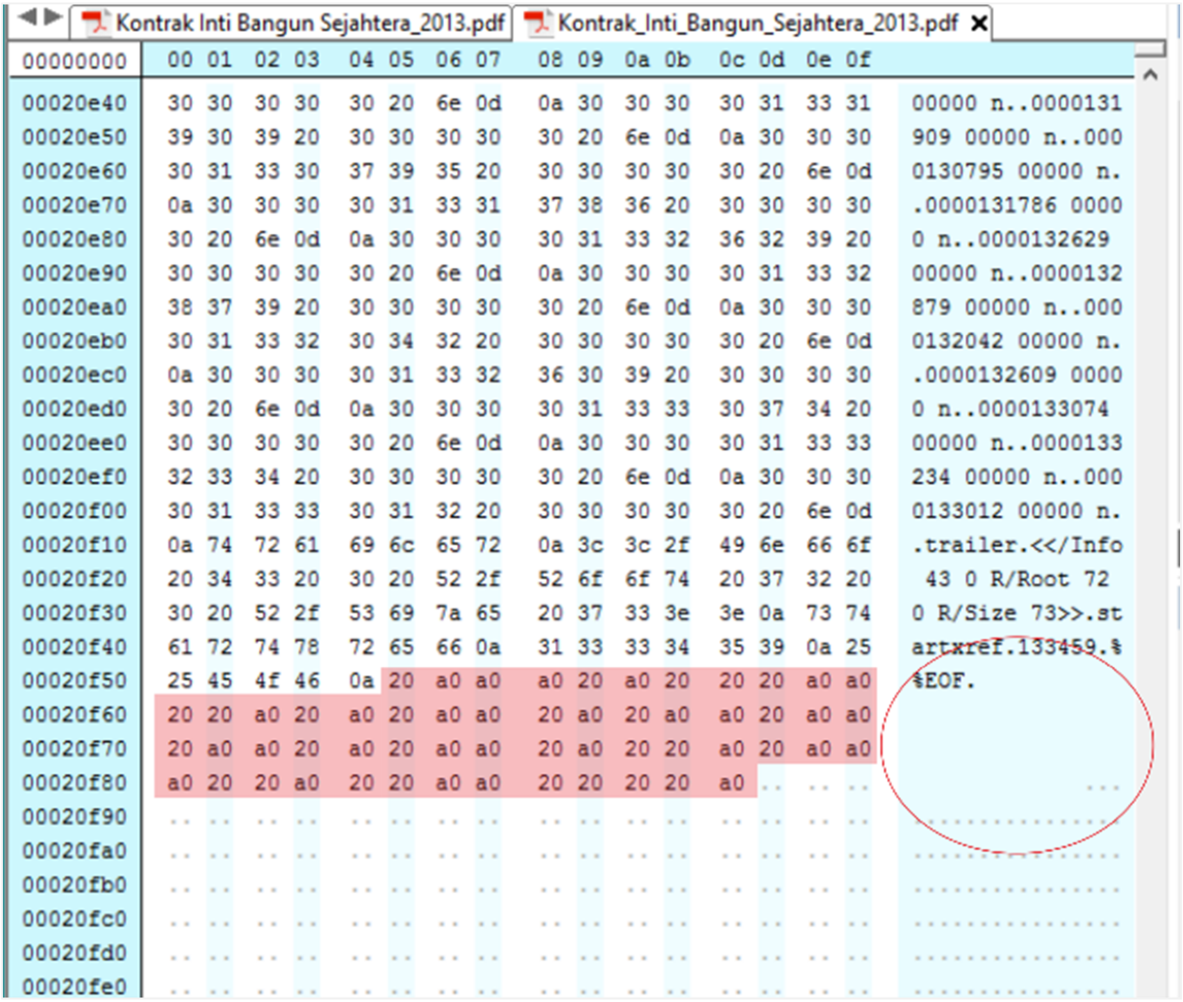
h. CLA encrypt validation ID with CLA key.

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.
p. Client revceive request. Verify current session.
q. CLA and CTF melakukan check current session validation ID.
r. CLA and CTF validation ID matched.
s. Client show dashboard page.

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.



Kontrak Inti Bangun Sejahtera_2013.pdf
Kontrak_Inti_Bangun_Sejahtera_2013.pdf

```
00000000   00 01  02 03   04 05  06 07   08 09  0a 0b   0c 0d  0e 0f
00020e40   30 30  30 30   30 20  6e 0d   0a 30  30 30   30 31  33 31   00000 n..0000131
00020e50   39 30  39 20   30 30  30 30   30 20  6e 0d   0a 30  30 30   909 00000 n..000
00020e60   30 31  33 30   37 39  35 20   30 30  30 30   30 20  6e 0d   0130795 00000 n.
00020e70   0a 30  30 30   30 31  33 31   37 38  36 20   30 30  30 30   .0000131786 0000
00020e80   30 20  6e 0d   0a 30  30 30   30 31  33 32   36 32  39 20   0 n..0000132629
00020e90   30 30  30 30   30 20  6e 0d   0a 30  30 30   30 31  33 32   00000 n..0000132
00020ea0   38 37  39 20   30 30  30 30   30 20  6e 0d   0a 30  30 30   879 00000 n..000
00020eb0   30 31  33 32   30 34  32 20   30 30  30 30   30 20  6e 0d   0132042 00000 n.
00020ec0   0a 30  30 30   30 31  33 32   36 30  39 20   30 30  30 30   .0000132609 0000
00020ed0   30 20  6e 0d   0a 30  30 30   30 31  33 33   30 37  34 20   0 n..0000133074
00020ee0   30 30  30 30   30 20  6e 0d   0a 30  30 30   30 31  33 33   00000 n..0000133
00020ef0   32 33  34 20   30 30  30 30   30 20  6e 0d   0a 30  30 30   234 00000 n..000
00020f00   30 31  33 33   30 31  32 20   30 30  30 30   30 20  6e 0d   0133012 00000 n.
00020f10   0a 74  72 61   69 6c  65 72   0a 3c  3c 2f   49 6e  66 6f   .trailer.<</Info
00020f20   20 34  33 20   30 20  52 2f   52 6f  6f 74   20 37  32 20    43 0 R/Root 72
00020f30   30 20  52 2f   53 69  7a 65   20 37  33 3e   3e 0a  73 74   0 R/Size 73>>.st
00020f40   61 72  74 78   72 65  66 0a   31 33  33 34   35 39  0a 25   artxref.133459.%
00020f50   25 45  4f 46   0a 20  a0 a0   a0 20  a0 20   20 20  a0 a0   %EOF.
00020f60   20 20  a0 20   a0 20  a0 a0   20 a0  20 a0   a0 20  a0 a0
00020f70   20 a0  a0 20   a0 20  a0 a0   20 a0  20 20   a0 20  a0 a0
00020f80   a0 20  20 a0   20 20  a0 a0   20 20  20 20   a0 ..  .. ..              ...
00020f90   .. ..  .. ..   .. ..  .. ..   .. ..  .. ..   .. ..  .. ..   ................
00020fa0   .. ..  .. ..   .. ..  .. ..   .. ..  .. ..   .. ..  .. ..   ................
00020fb0   .. ..  .. ..   .. ..  .. ..   .. ..  .. ..   .. ..  .. ..   ................
00020fc0   .. ..  .. ..   .. ..  .. ..   .. ..  .. ..   .. ..  .. ..   ................
00020fd0   .. ..  .. ..   .. ..  .. ..   .. ..  .. ..   .. ..  .. ..   ................
00020fe0   .. ..  .. ..   .. ..  .. ..   .. ..  .. ..   .. ..  .. ..   ................
```

Figure 9. Insertion result using whitespace manipulation

Matched Validation ID	d16639200901bbbc5509da7b8613cb00
Decrypted Validation ID	3177835804342202
Validation ID on CLA	d16639200901bbbc5509da7b8613cb00
Validation ID on CTF	63d3964f83d2be34669829f6ae6116f6

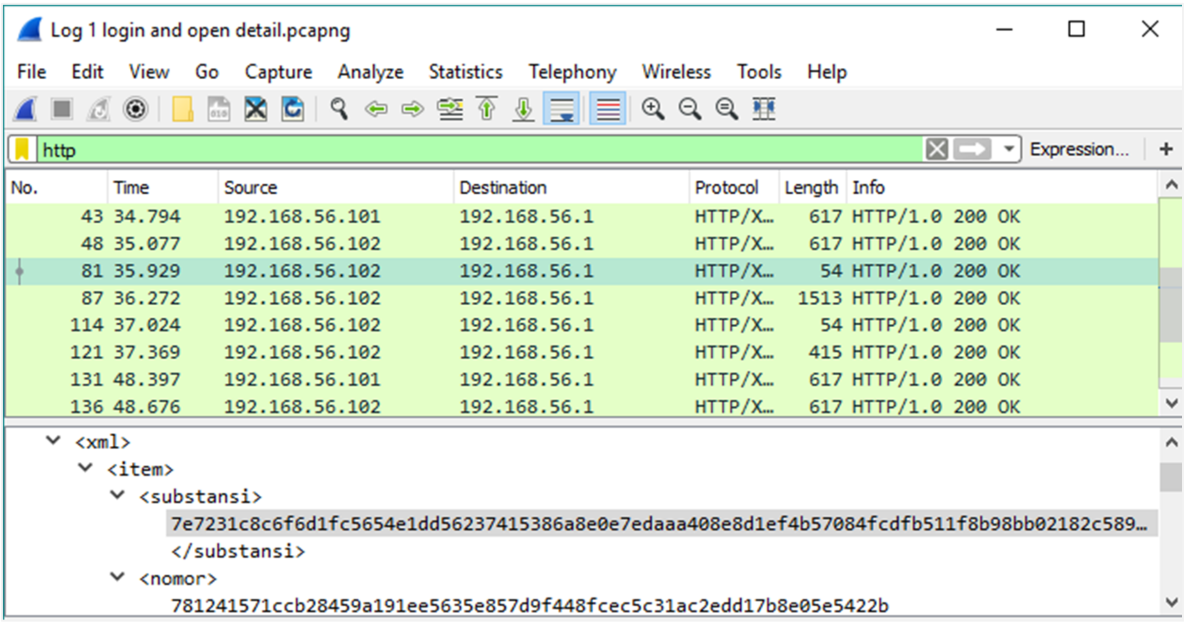
Figure 10. Validation ID matching

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)


Log 1 login and open detail.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+

```
No.   Time    Source          Destination    Protocol  Length Info
   43 34.794  192.168.56.101  192.168.56.1   HTTP/X…     617 HTTP/1.0 200 OK
   48 35.077  192.168.56.102  192.168.56.1   HTTP/X…     617 HTTP/1.0 200 OK
   81 35.929  192.168.56.102  192.168.56.1   HTTP/X…      54 HTTP/1.0 200 OK
   87 36.272  192.168.56.102  192.168.56.1   HTTP/X…    1513 HTTP/1.0 200 OK
  114 37.024  192.168.56.102  192.168.56.1   HTTP/X…      54 HTTP/1.0 200 OK
  121 37.369  192.168.56.102  192.168.56.1   HTTP/X…     415 HTTP/1.0 200 OK
  131 48.397  192.168.56.101  192.168.56.1   HTTP/X…     617 HTTP/1.0 200 OK
  136 48.676  192.168.56.102  192.168.56.1   HTTP/X…     617 HTTP/1.0 200 OK
```

```
<xml>
  <item>
    <substansi>
      7e7231c8c6f6d1fc5654e1dd56237415386a8e0e7edaaa408e8d1ef4b57084fcdfb511f8b98bb02182c589…
      </substansi>
    <nomor>
      781241571ccb28459a191ee5635e857d9f448fcec5c31ac2edd17b8e05e5422b
```

Figure 11. Capture result using wireshark

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

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.

Tabel 4. Turn around time result

No	File Name	File Size (in KB)	Time (in second)		
			Encrypt	Decrypt	Total
1	Daftar_KS_Kelitbangan_tekmira_2012-2013.PDF	14	2.173	8.008	10.181
2	Kerjasama_LN_2006-2010.PDF	16	2.118	9.239	11.357
3	D2L_Learning_Repository_Brochure.PDF	52	7.532	32.553	40.085
4	chen5.PDF	84	12.363	65.913	78.276
5	mathjournal94.PDF	92	12.891	58.344	71.235
6	Rencana_PT_Smelting_14_April.PDF	131	21.992	79.884	101.876
7	Kontrak_Inti_2013.PDF	132	20,973	81,788	102,761
8	Daftar_KS_tekmira_Korea_ongoing_2010-2012.PDF	171	23.401	108,33	131,731
9	Perjanjian_Kerjasama_Kemitraan_Litbang_2006-2014.PDF	176	26,443	115,655	142,098
10	Daftar_KS_DN_KESDM_2006-2012.PDF	206	28.462	135,216	163,678
11	Daftar_KS_tekmira_2010-2012.PDF	219	30,323	142,922	173,245
12	automatic_format_identification.PDF	250	37,243	173,657	210,900
13	Daftar_KS_tekmira_Jepang.PDF	292	46,431	183,736	230,167
14	SecureOnlineVoting.PDF	297	44,482	206,178	250,66
15	Analysis of LSB based Image Steganography Techniques.PDF	325	49,011	209,225	258,236
16	fmipa2012016.PDF	374	57,601	267,616	325,217
17	Schneier.PDF	402	61,005	255,226	316,231
18	Kontrak_Pelayanan_Jasa_2006-2014.PDF	413	58,057	263,158	321,215
19	Draft_PT_Smelting_15_April.PDF	432	62,423	274,466	336,889
20	DK21713717.PDF	508	76,699	325,088	401,787
21	dct.PDF	595	88,962	385,769	474,731
22	Chapter II.PDF	702	104,508	462,911	567,419
23	271332100014.PDF	755	109,941	483,805	593,746
24	spread_spectrum_image_steganography.PDF	906	132,747	577,424	710,171
25	Universal Algorithm.PDF	1003	142,988	633,531	776,519

5.3. Two Central FacilitiesProtocol Impelemntation Analysis

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 wheter 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, authetication, 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 integirty 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.

Table 5. Comparison of single and two central facilities

	Single Central Facilities	***Two Central Faciliites***
Confidentiality	Data on transmission can be sniffed by irresponsible party. Confidentiality aspect is not fulfilled.	Data on transmission can be sniffed by irresponsible party. Confidentiality aspect is not fulfilled.
Authentication	There is no addition rule to authenticate user. Authentication aspect is not fulfilled.	There is addition rules to authenticate user. Authentication aspect is fulfilled.
Anonymity	Anonymity is not provided. Anonymity aspect is fulfilled.	Anonymity is not provided. Anonymity aspect is fulfilled.
Non-repudiation	System record user's activity. Sistem mencatat aktivitas user. Non-repudiation aspect is fulfilled.	System record user's activity. Sistem mencatat aktivitas user. Non-repudiation aspect is fulfilled.

Table 6. User authentication

Type	**Quantity**	**Note**
Number of authorized user	21	Specific staff of PUSLITBANG tekMIRA
Number of unauthorized user	147	Rest of the staff
Total	168	

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 predefine 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

Al-Othmani, A. Z. M. (2009). *Prototype development of VOIP steganography* (Doctoral dissertation, Universiti Teknologi Malaysia).

Cheminod, M., Durante, L., & Valenzano, A. (2013). Review of security issues in industrial networks. *IEEE transactions on industrial informatics*, *9*(1), 277-293.

De Vivo, M., de Vivo, G. O., & Isern, G. (1998). Internet security attacks at the basic levels. *ACM SIGOPS operating systems review*, *32*(2), 4-15.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on information theory*, *22*(6), 644-654.

Hurd, P. D. (1998). Scientific literacy: New minds for a changing world. *Science education*, *82*(3), 407-416.

Lambrinoudakis, C., Gritzalis, S., Dridi, F., & Pernul, G. (2003). Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. *Computer communications*, *26*(16), 1873-1883.

Liao, Y. P., & Hsiao, C. M. (2014). A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. *Ad hoc networks*, *18*, 133-146.

Muharram, A. T., & Satrya, F. (2016). Rancang bangun sistem e-voting menggunakan protokol two central facilities. *Jurnal informatika*, *15*(1), 33-44.

Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. *Proceedings of the IEEE*, *87*(7), 1062-1078.

Por, L. Y., Ang, T. F., & Delina, B. (2008). Whitesteg: a new scheme in information hiding using text steganography. *WSEAS transactions on computers*, *7*(6), 735-745.

Potlapally, N. R., Ravi, S., Raghunathan, A., & Jha, N. K. (2006). A study of the energy consumption characteristics of cryptographic algorithms and security protocols. *IEEE transactions on mobile computing*, *5*(2), 128-143.

Sartor, G. (2013). Providers' liabilities in the new EU data protection regulation: A threat to internet freedoms?. *International data privacy law*, *3*(1), 3-12.

Sharma, D. K., Pathak, V. K., & Sahu, G. P. (2007). Digital watermarking for secure e-government framework. *Computer society of india*, *7*, 182-191.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM sigmis database*, *38*(1), 60-80.

Sullivan, K., Griswold, W. G., Rajan, H., Song, Y., Cai, Y., Shonle, M., & Tewari, N. (2010). Modular aspect-oriented design with XPIs. *ACM transactions on software engineering and methodology*, *20*(2), 5.

Sun, J., Liu, B. Y., McMurry, P. H., & Greenwood, S. (1994). A method to increase control efficiencies of wet scrubbers for submicron particles and particulate metals. *Air and waste*, *44*(2), 184-194.

Thakur, J., & Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. *International journal of emerging technology and advanced engineering*, *1*(2), 6-12.