Development of Front-End And Implementation of AES Encryption Algorithm on Solidare Mobile Apps

Muhammad Iqbal Tawaqal[1]

[1] Informatics Engineering – Universitas Komputer Indonesia
Dipatiukur street 112-114 Bandung
Email : iqbal.tawakal@*outlook*.com[1]

ABSTRACT

An annual article 2013 UNICEF stated that there are approximately 2.3 million children age 7-15 years are Indonesian children who drop out from school. Rumah Zakat is charity organization whose purpose is to be a facilitator connecting donors donate to children who drop out from school. However, there are so many problems in implementation such as from the donor regarding the difficulty making children recommendation, selection of out of school children, and knowing the development of children that has been donated. And from society regarding the difficulty in obtaining information about out of school children and how to help them, and also regarding the confidentiality of data from charity organization/social communities. The solution can be applied to the problems is to build front-end Solidare mobile app.

The research methodology that used in development of front-end application is method applied research. The first step of development is analyzing all the problems, and then analyzing system architecture, further analyzing the encryption aes-128 algorithm that used for data security, and collect all the application needs to be used as material for the analyze of application functionality. After that perform system design frontend.

Solidare frontend application that has been designed and then implemented in the programming language C# on windows phone platform. And continued testing of the system by using black box method and beta testing. Results of the testing showed that the front-end system application has been easier for donors/societies in obtaining information about out of school children, making a donation, do a recommendation to out of school children, and applying the encryption AES-128 algorithm in order to maintain the confidentiality of the data on the system front-end applications.

Key words: Donation Application, Windows Phone, Children, Enryption Algorithm, AES.

1. PENDAHULUAN

Education and poverty are the two things are closely related to its influence in the center of social life. This can be seen in the annual article 2013 of UNICEF to Indonesia entitled "The Story Of Indonesia" can be the fact that there are approximately 2.3 million children aged 7-15 years or 42% of Indonesia's population are mostly school dropouts [1] , Economic factors are the main cause of school dropouts, reaching 36%. Overcome this, the charity has had the legality of legally present and answer these problems by helping the children out of school. Yayasan Rumah Zakat Indonesia come to give solution to children dropping out of school by providing assistance in the form of scholarships and some scholarships to the needs of school supplies and other scholarship programs. The goal is as a facilitator connecting donors donate to children who drop out of school.

Based on observations with part scholarships at the headquarters of the Foundation RZ obtained some of the facts which are the donors is difficult to get information on the activities / news of the latest social communities or of charity. The difficulty donors make donations to other foster care because of the unavailability of data presentation foster children even provide options to suit the wishes of donors. In addition, donors difficulty if you want to recommend the school dropouts who are in the surrounding environment and the general public still having trouble getting information about underprivileged kids / children dropping out of school and how to help them.In addition to some of the facts and problems, in a good mobile application development begins to consider what kind of data security that is used. In this study, the data security in mobile applications Solidare algorithm using Advanced Encryption System (AES) [2].Then the mobile device selection in this study is because mobile devices are expected to dominate the market up to 2.16 billion in the year 2016 with a growth rate of 12.6% from 2015 [3].

1.1 Metode Pembangunan Perangkat Lunak

Software development method used in the construction of Solidare frontend that waterfall models. The following process is the waterfall model [4]:

1. Requirements analysis and definitionCollection needs have been defined in full and then analyzed and defined needs that must be met by the program to be built.
2. System and software designDoing design software. Done after the completion requirements are collected in full.
3. Implementation and unit testingResults of the program design is translated into codes by using a programming language that has been determined. The program is built directly tested by its units.
4. Integration and system testingUnification of the program units then tested the system as a whole.
5. Operation and maintenanceOperate the program in their environment and perform maintenance, such as adjustment or change because adaptation to the actual situation.Here are the stages of software development with the waterfall model can be seen in Figure I 1 the following:

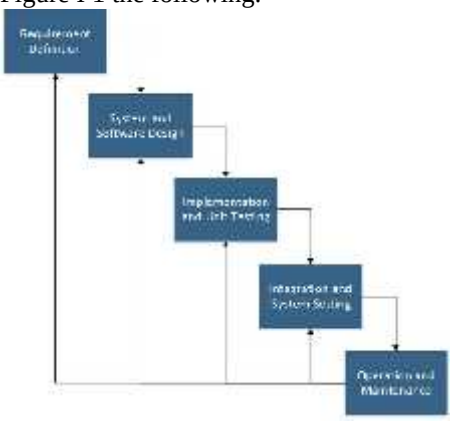


Figure I 1 Model Waterfall

1.2 Citizen Journalism

The basic concept of citizen journalism that is positioned in the audience as a news producer as well, not just passive consumers as long as it goes in the logic of traditional journalism work-based media. That is the position of the journalist as a search and news writer, speaker as a source of news, and the audience as consumers of news is not valid. Between producer and consumer news can no longer be identified in detail because anyone can play both. In essence, the citizen journalism that takes precedence is the active role undertaken by the community in the activities of collecting, reporting, analyzing and delivering information and news [5].

II.1 *Advanced Encryption Standard*

Advanced Encryption Standard is a symmetric cryptographic algorithm that can be used to secure the data. This is a standard encryption algorithm with a key-symmetrical. AES algorithm with a symmetric block cipher text can encrypt (encipher) and decryption (decipher) the information. This type of algorithm is divided into three, namely AES-128, AES-192 and AES-256. Each type of the AES algorithm can encrypt and decrypt data at block 128 bits, 128 bits block is a fixed size block cipher used in the AES algorithm. Block cipher has the following characteristics:

a. Plaintext is divided into blocks of bits with the same length, for example 128 bits.
b. An encryption key length = length of the block
c. Encryption is done on the bit plaintext block using key bits.
d. Encryption algorithms produce ciphertext block length = block of plaintext.

1.3 JSON

JSON (*JavaScript Object Notation*) adalah format pertukaran data yang ringan, mudah dibaca dan ditulis oleh manusia, serta mudah diterjemahkan dan dibuat (*generate*) oleh komputer. JSON sendiri memiliki struktur data yang terdiri dari *json array* dan *json object*. *Json array* adalah kumpulan nilai yang terurutkan dan memiliki bentuk kurung kotak ([ ]), sedangkan *json object* adalah kumpulan pasangan *string* dan *value* dan memiliki bentuk kurung kurawal ({ }) [9].

1.4 Pemrogramman Berorientasi Objek

Object-oriented programming (PBO) is a continuation of the process of object-oriented analysis and design. In the object-oriented programming, component designed in the design process is implemented using object-oriented programming language. Here are some of the object-oriented programming concepts, namely:1. ObjectsIn the PBO, the object is a composition / framework in the form of data and procedures to operate the data.2. AbstractionAbstraction is representative of data or the same procedure to conceal an object if it is not connected and can be used in other cases if they relate.3. EncapsulationEncapsulation is a process that does not allow direct access to the data (data hidden). In order to access the data, it must first be connected to the object responsible for the data.4. PolymorphismPolymorphism is the ability of two different objects in response to the same request in its own way.5. InheritanceInheritance (inheritance) is used to classify objects in the program based on common characteristics.6. AggregationAggregation is the condition when an object is combined with part of another object, and then work together.

1.5 *Unified Modelling Language* (UML)

Unified Modeling Language (UML) is a standard modeling language used in software development with object oriented approach. In designing the system, the model has an important role to manage complexity. Modeling can connect every important aspect of system design. A model is a representation of a real object. Models are built is the simplification of the system to be built. Model gives purpose and viability of the system to be understood and evaluated. And provide insight faster than should directly into the actual system. UML version 2.0 has a 13 diagram that can be used. However, in this study only 4 UML diagram that will be used. Table II 1 explains the diagram that will be used.

Table II 1 UML 2.0 diagrams are Used

Nama Diagram	Deskripsi
Use Case Diagram	Describe the interaction between user and system to be built. Assist in mapping the needs of the system. Illustrates the sequential and parallel activity in the system. Describes the relationship classes, interfaces in the system. Describe interactions between objects in which the order of each object and its interaction is very important.
Activity Diagram	Describe the interaction between user and system to be built. Assist in mapping the needs of the system. Illustrates the sequential and parallel activity in the system. Describes the relationship classes, interfaces in the system. Describe interactions between objects in which the order of each object and its interaction is very important.
Class Diagram	Describe the interaction between user and system to be built. Assist in mapping the needs of the system. Illustrates the sequential and parallel activity in the system. Describes the relationship classes, interfaces in the system. Describe interactions between objects in which the order of each object and its interaction is very important.
Sequence Diagram	Describe the interaction between user and system to be built. Assist in mapping the needs of the system. Illustrates the sequential and parallel activity in the system. Describes the relationship classes, interfaces in the system. Describe interactions between objects in which the order of each object and its interaction is very important.

2. ISI PENLITIAN

2.1 Problem Analysis

Here are some of the problems that arise in this study are:

1. The difficulty of donors to recommend underprivileged children because of the limited knowledge about the information / how to recommend to social communities or charities.
2. The difficulty of donors to donate to underprivileged children / other school dropouts due to the unavailability of data presentation underprivileged child / children out of school even gives the option accordance with the wishes of donors.
3. The difficulty of donors to determine a child's development because of the lack of services that allows donors to get reports of child development that terdonasi.
4. The general public is sometimes difficult to get information about underprivileged kids / children

dropping out of school and do not know how menbantu them.
Important data from the data foundation and donors who are internal and confidential, so it is necessary to implement security on the data.

2.2 Frontend System Architecture

Solidare frontend system architecture can be seen in *Figure* III 1.

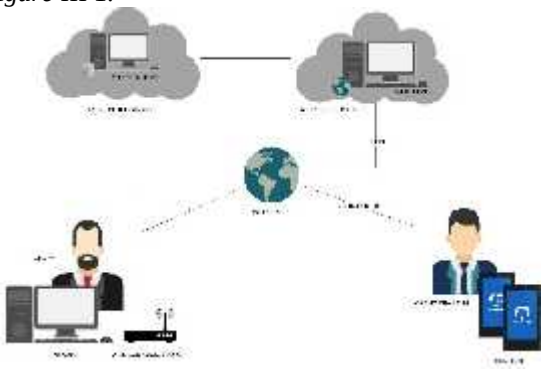


Figure 0-1 *Solidare frontend system architecture*

General overview of the system architecture consists of two subsystems. The first is where the web administrator is an administrator to manage the website that has been stored in the web server hosting and cloud computing services Microsoft Azure Web Service. Once saved, in this administrator also provided web service API in the form of charity so that data can be accessed by other platforms. Encode the data form the results of its PHP is JSON. The second is the windows phone mobile devices where the data will be in the form of JSON-parsing the JSON parser so that data from the web administrator can be accepted by donors.

2.3 Analyze of AES Encryption Agorithm

On this analysis will be explained how the cryptographic algorithm implemented into Solidare frontend systems. Cryptographic algorithms used in cryptographic algorithms frontend Solidare is 128 Bit Advanced Encryption Standard (AES-128). In the AES-128 algorithm, there are two processes, namely the processes of encryption and decryption process

2.4 Architecture Design Frontend

Here is the architectural design frontend menu Solidare:

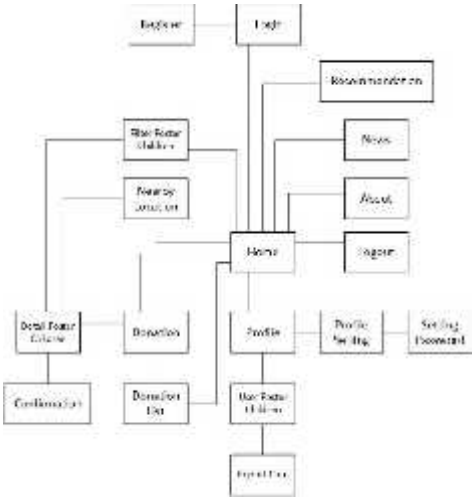


Figure 0-2 design frontend menu Solidare

2.5 Design Of Message

The design of the message that will be discussed is the design of an existing message on frontend Solidare. Here are some messages on frontend design Solidare.

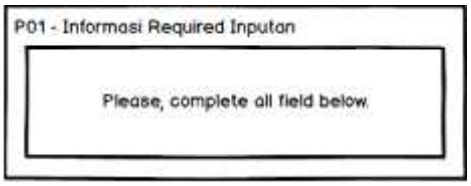


Figure 0-3 *P01-Required Input Data*

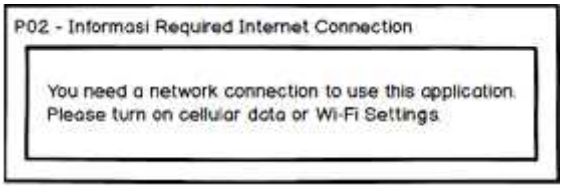


Figure 0-4 P02-Informasi *Required Internet Connection*

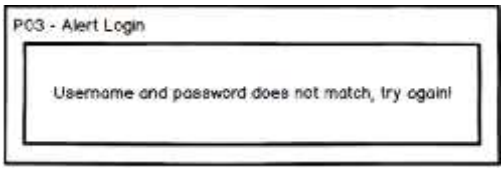


Figure 0-5 *P03-Alert Login*

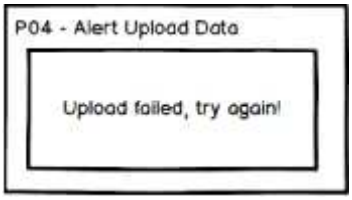


Figure 0-6 *P04-Alert Upload Data*

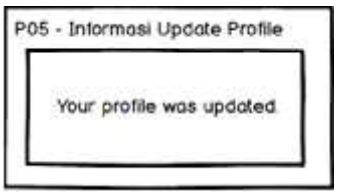


Figure 0-7 *P05-Informasi Update Profile*

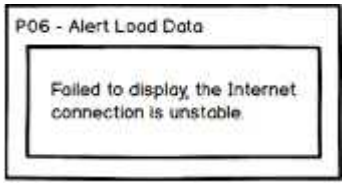


Figure 0-8 *P06-Alert Load Data*

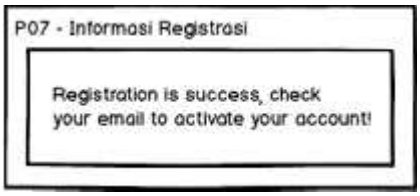


Figure 0-9 *P07-Informasi Registrasi*

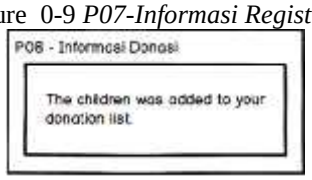


Figure 0-10 *P08-Informasi Donasi*

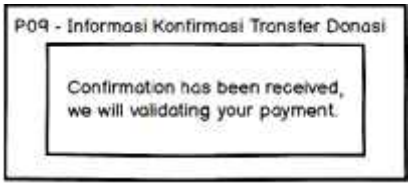


Figure 0-11 Informasi Konfirmasi Transfer Donasi

2.6 Semantic Network

Here is a semantic network of frontend Solidare.

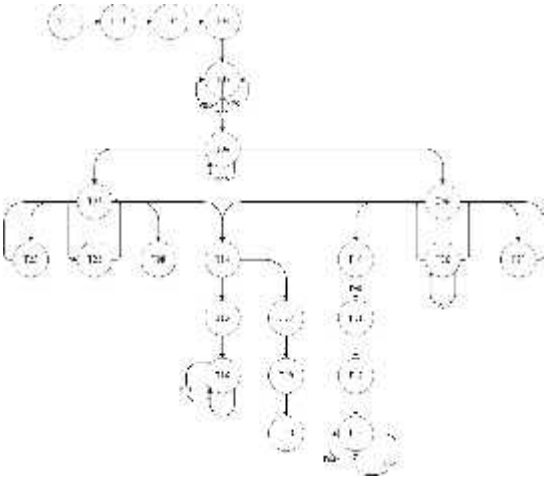


Figure 0-12 semantic network of frontend Solidare

2.7 Implementasi Sistem

Implementation of the system is done in this study is to describe the environment in which the system will be implemented / installed. Then the implementation of any interface design where any registered interfaces that are implemented later if it wanted to see a screenshot of it can be seen in the appendix Implementation environment is the specification of hardware, software where the system will be installed and used. Here is the implementation environment:

1. *Hardware Environment*

Here are the hardware specifications in the development of this software.

Table IV 1 Frontend Builders Hardware Implementation Environment Applications

No	Item	Spesifications
1	Processor	Intel Core i7-4510U CPU @ 2.00 GHz 2.60 GHz
2	Harddisk	1 TB
3	Memory	4 GB
4	VGA	4 GB
5	Monitor	14 inch
6	Mouse	Optical Microsoft Sculpt Touch
7	Keyboard	QWERTY Creative
8	USB port	3 port
9	Internet Connection	yes
10	Windows Phone 8.0	Phablet Lumia 1520 6 inch dan Lumia 520 4.5 inch

Here is specification for hardware to access the system:

Tabel 0-1 *Hardware Environment*

No	Item	Spesifikasi
1	Processor	@ Dual-Core 1 GB
2	SD Card	8 GB
3	Memory	512 GB
4	Koneksi Internet	Ada
5	Windows Phone version	8.0

1. *Software Environment*

The software used in the construction of this Solidare frontend is:

1. Operating System Windows 8 64-bit Single Language.
2. The programming language C #.
3. Code editor using Microsoft Visual Studio 2013 Community Update 4.
4. Windows phone applications built using the .NET Framework 4.
5. The exchange of data is done using JSON..

Here is specification for Software to access the system:

Table 0-2 Software Environment

No	Item	Spesifikasi
1.	Windows Phone version	8.0 (Lumia Denim)

IV.1.1 Implementation of UI

This section contains the interface implementation of windows phone in which the implementation of the interface is represented by interface name along with the name of the file they represent.

Table 0-3 UI Implementation

No	Nama Antarmuka	Nama File
1	Walkthrough Aplikasi	PageStart.xaml
2	Login	PageLogin.xaml
3	Register	PageRegister.xaml
4	Timeline News	NewHomepage.xaml
5	Detail News	PageDetailNews.xaml
6	Timeline Donation	NewHomepage.xaml
7	Profile	PageProfileDonatur.xaml
8	User Sponsored Children	PageProfileDonatur.xaml
9	Report Card	PageRapotAnak.xaml
10	Detail Profile	PageDetailDonatur.xaml
11	Setting Profile	PageSetting.xaml
12	User Change Password	PagePassword.xaml
13	Children Recommendation	PageRekomendasi.xaml
14	Detail Children	PageDetailAnak.xaml PageProfileAnak.xaml DetailAnakAsuhNearby.xaml
15	Donation List	PageKeranjangDonasi.xaml
16	Donation Detail	DetailDonation.xaml
17	Confirmation	PageKonfirmasi.xaml
18	Filter Children	PageFilter.xaml
19	Nearby Location	PageNearby.xaml
20	About	PageAbout.xaml
21	Terms & Conditions	PageTerms.xaml

From the list above table, it can be concluded that the entire interface has been implemented in the class. For details of its interface can be found in appendix A.

2.8 System Testing

Testing the frontend system consists of two stages of testing alpha and beta testing. The method used in this frontend system testing method is to use black box testing where this test focuses on the functional requirements of the software. In the test scenario is divided into two types, namely functional test scenarios and test scenarios acceptance.

1. Scenario functional testing Scenario functional testing is done by testing one frontend system is windows phone. Scenario testing frontend windows phone system can be seen in Table IV 5.

Table 0-4 Functionall testing scenario

No	Kelas Uji	Poin Pengujian	Jenis Pengujian
1	*Login*	Isi data *login*	*Equivalence Partitioning*
		Validasi *field login*	*Equivalence Partitioning*
2	*Register*	Isi data register	*Equivalence Partitioning*
		Validasi *field register*	*Equivalence Partitioning*
3	*Forgot password*	Memasukan *email* dan nomor telepon	*Equivalence Partitioning*
		Validasi *field email* dan *nomor telepon*	*Equivalence Partitioning*
4	*Setting profile*	Isi data *profile*	*Equivalence Partitioning*
5	*Change password*	Memasukan *current-password* dan *new-password*	*Equivalence Partitioning*
		Validasi *field current-password* dan *new-password*	*Equivalence Partitioning*
6	*Donation*	Memililh anak yang akan didonasi	*Equivalence Partitioning*
7	*Confirmation* transfer donasi	Isi data *confirmation*	*Equivalence Partitioning*
		Validasi *field confirmation*	*Equivalence Partitioning*
9	Rekomendasi anak	Isi data rekomendasi anak	*Equivalence Partitioning*
11	Filtering anak berdasarkan status anak	Memilih status *orphan, orphans,* dan *poor children.*	*Equivalence Partitioning*
12	Filtering anak berdasarkan jenjang pendidikan anak	Memilih jenjang pendidikan *elementary school, junior school,* dan *high school.*	*Equivalence Partitioning*

13	Filtering anak berdasarkan jenis kelamin anak	Memilih jenis kelamin anak laki-laki dan perempuan.	*Equivalence Partitioning*

1. Skenario pengujian beta

Berikut adalah daftar pertanyaan kuesioner pengujian beta yang disebar kepada 30 masyarakat sabagai calon pengguna *frontend* aplikasi yang dibangun yang dapat dilihat pada Tabel 0-5.

Tabel 0-5 Daftar Pertanyaan Kuesioner

NO	PERTANYAAN	SS	S	N	T	ST	Metode Hasil Pengujian
1	Apakah anda setuju jika daftar anak kurang mampu/anak putus sekolah ditampilkan pada aplikasi ini?						
2	Apakah anda setuju aplikasi ini memberikan kemudahan untuk merekomendasikan anak kurang mampu/anak putus sekolah?						
3	Apakah anda setuju aplikasi ini membantu dalam berdonasi?						
4	Apakah anda setuju aplikasi ini memberikan kemudahan dalam melakukan konfirmasi transfer donasi?						Skala *Likert*
5	Apakah anda setuju aplikasi ini memberikan *feedback* laporan perkembangan anak setiap semesternya?						
6	Apakah anda setuju tampilan aplikasi ini mudah dipahami?						
7	Apakah anda setuju jika pada sebuah aplikasi *mobile* hanya memiliki satu warna dominan?						
8	Apakah anda setuju jenis *font* pada aplikasi ini mudah untuk dibaca?						
9	Apakah anda setuju ukuran *font* pada aplikasi ini sesuai untuk dibaca?						
10	Apakah anda setuju dengan adanya keamanan data pada aplikasi ini?						

The test results are the result of test scenarios that have been developed previously. Results of tests performed consisted of the results of the testing and beta testing functionality.

3. CONCLUSION

Based on test results Solidare frontend application on windows phone platform, it can be concluded the following

1. Frontend Solidare application on windows phone platform has largely been able to facilitate the donor in making donations to underprivileged children / school dropouts.
2. Frontend Solidare application on windows phone platform has largely been able to facilitate donors in making recommendations underprivileged child / children out of school are located around the user's environment.
3. Frontend Solidare application on windows phone platform has largely been able to facilitate donors in getting reports of child development that has terdonasi by the user.
4. Frontend Solidare application on windows phone platform has largely been able to help people as a medium of information about the news of the social community / charity and as a medium to donate to underprivileged child / children out of school.
5. Frontend Solidare application on windows phone platform has been using AES-128 encryption algorithm in the process of exchanging data with the web server. So that data encrypted with both and reduce the possibility of data intimidation from outsiders who are not responsible.

4. REFERENCES

[1] Laporan Tahunan Indonesia, UNICEF, 2013.

[2] “Advanced Encryption Standard,” 25 November 2014. [Online]. Available: https://id.wikipedia.org/wiki/Advanced_Encryption_Standard. [Diakses 5 July 2015].

[3] “Mobile App Developers: Start with Security,” February 2013. [Online]. Available: https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security. [Diakses 5 July 2015].

[4] Z. Habibi, “"Citizen Journalism": Ketika Berita Tidak Hanya Memiliki Satu Muka,” *Jurnal Komunikasi*, vol. 1, no. 2, pp. 1-18, 2007.

[5] j. org, “json org,” [Online]. Available: http://json.org/json-id. [Diakses 5 July 2015].

[6] I. Sommerville, Software Engineering, USA: Pearson Education, Inc., 2011.

[7] Ayushi, “Symmetric Key Cryptographic Algorithm,” *International Journal of Computer Applications*, vol. 1, no. 1, pp. 1-4, 2010.

[8] C. Ireland, B. David, M. Newton dan K. Waugh, “Understanding Object-Relational Mapping: A Framework Based Approach,” *International Journal on Advances in Software,*, vol. 2 no. 2&3, pp. 202-216, 2009.

[9] P. Pramudya, Membuat Aplikasi untuk Windows Phone, Bandung: ANDI, 2011.

[10] J-LAB, “J-LAB Knight Community News Network,” Knight Foundation, [Online]. Available: http://kcnn.org/learning-modules/principles-of-citizen-journalism/. [Diakses 10 Agustus 2015].

[11] D. Selent, “Advanced Encryption Standard,” *InSight: RIVER ACADEMIC JOURNAL*, vol. 6, no. 2, pp. 1-14, 2010.