MOBILE BANKING SYSTEM DEVELOPMENT USING NEAR FIELD COMMUNICATION TECHNOLOGY WITH ANDROID-BASED OPERATING SYSTEM (CASE STUDY: PT. BANK PANIN SYARIAH TBK)

Bisri Nursa Fadillah[1], Dewi Khairani[2], Nurul Faizah Rozy[3]

[1,2,3]Informatics Engineering, Science and Technology Faculty
UIN Syarif Hidayatullah
bisrinursa@gmail.com, dewi.khairani@uinjkt.ac.id, nurulfaizah200@gmail.com

ABSTRAK

Pengembangan teknologi informasi (TI) digunakan untuk mendukung sektor bisnis, termasuk perbankan. Salah satunya, perbankan menggunakan IT untuk meningkatkan kualitas layanan dalam bentuk *internet banking* dan *mobile banking*. Oleh karena itu, penelitian ini berfokus pada pengembangan sistem *mobile banking* menggunakan teknologi *Near Field Communication* (NFC) sebagai otentikasi klien dan sistem keamanan. Fitur pada sistem *mobile banking* adalah memeriksa informasi saldo, mutasi, tagihan listrik, transfer sesama bank dan transfer antara Bank yang telah bekerja dengan ATM Bersama, serta pembayaran tagihan listrik. Pengembangan sistem menggunakan bahasa pemrograman JAVA dengan alat *Android Studio*, untuk mengakses *server* menggunakan PHP dengan MySQL sebagai manajemen basis data, IdWebHost sebagai layanan *hosting*, serta output data menggunakan format JSON. Metode pengumpulan data dilakukan dengan tahap wawancara dan studi literatur. Peneliti menggunakan metode pengembangan sistem *Rapid Application Development* (RAD), sedangkan pengujian menggunakan pengujian unit dan pengujian penerimaan pengguna. Hasil dari penelitian ini adalah sistem *mobile banking* yang aman menggunakan teknologi *Near Field Communication*, PIN, dan enkripsi AES.

Kata Kunci: *Mobile Banking, Near Field Communication, Android, Cryptography, AES*

ABSTRACT

Development of information technology (IT) is used to support business sector, including banking. One of them, banking uses IT to improve the quality of service in the form of internet banking and mobile banking. Therefor, the research focused on development of mobile banking system using Near Field Communication (NFC) technology as client authentication and security system. Features on mobile banking system are checking balance information, mutation, electricity bill, a fellow bank transfer and transfers between Bank that has been working with ATM Bersama, as well as payment of electricity bills. System development using JAVA programming language with Android Studio tools, to access server using PHP with MySQL as database management, IdWebHost as hosting services, as well as data output using JSON format. Data collection method is done with interview stage and literature study. Researcher uses system development methods of Rapid Application Development (RAD), while testing using unit testing and user acceptance testing. Result of the study is secure mobile banking system utilizing Near Field Communication technology, PIN, and AES encryption.

Keywords: *Mobile Banking, Near Field Communication, Android*

I. INTRODUCTION

Development in information technology should be able to support business areas, including banking business, as regulated in Law Number 10 Article 2 Year 1998 on Amendment of Law Number 7 Year 1992 concerning Banking declare the main function of Indonesian banking is as collector and distributor of society's funds. In carrying out these functions, banking business needs information technology such as internet banking and mobile banking.

Referring to the research results of Kadence International [1] regarding preference pattern banking customer to Banking E-Channel service conducted on November 21 to December 11, 2013, involving 453 respondents in four major cities in Indonesia: Jakarta, Medan, Makassar and Surabaya found that mobile banking is types of banking services most used by customer (67%), followed by internet banking (54%), and phone banking (28%). Meanwhile, based on survey conducted by Sharing Vision to the 8 major banks in Indonesia and according to various sources, the number of mobile banking users has reached approximately 19.9 [2].

Currently, mobile banking is growing because the service is able to provide the flexibility and practicality of transaction with the most basic features such as checking balance, pay bills, money transfer. This is supported by research conducted by [3] suggesting that banks are placing as much effort on digital marketing and tools as traditional brands.

The mobile banking concept that has been applied to the Bank in Indonesia, such as BCA Bank using Internet lines (GPRS / EDGE / 3G / WIFI) combined with Short Message Services (SMS) media, (BCA). Meanwhile, mobile banking that applied by BRI using SMS media. Smartphone consisting of several types are Android, Windows Phone, iOS, and Blackberry. Most Android smartphones in the market such as Samsung Galaxy S4, Samsung Galaxy Ace3 4G, and Sony Xperia SP has been attached Near Field Communication (NFC) technology. Growth in market share of the 4 types of smartphones is dominated by Android, as shown on Figure 1:

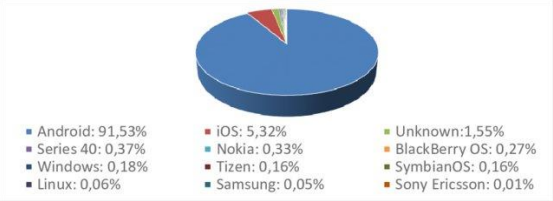

Figure 1. Operating system marketshare [4]

Referring to data from PT. Bank Panin Syariah Tbk, the company has 3000 customers and has 8 units ATM machine in 2014 spread in Jakarta, Surabaya, Bekasi, Surabaya, Malang, Tangerang, Bandung and Semarang as facilities for customer to perform a variety of transactions. The existence of customers who are not always located in 8 regions make the customer cannot make transactions such as money transfer transactions among fellow customers of PT. Bank Panin Syariah and between banks when outside Jakarta, Surabaya, Bekasi, Surabaya, Malang, Tangerang, Bandung and Semarang. Whereas PT. Bank Panin Syariah has mission to realize Islamic financial services in a professional, trustworthy and responsible and provide products and services with the best standards according to the customer's needs.

The adaptation of mobile banking and the security behind it has been a various studies among researcher, Madhoun [5] propose a solution that enhances the EMV protocol by adding a new security layer aiming to solve EMV weaknesses. We formally check the correctness of the proposal using a security verification tool called Scyther. Pourghomi [6] proposed protocol that eliminates the requirement of a shared secret between the Point-of-Sale (POS) and the Mobile Network Operator before execution of the protocol, a mandatory requirement in the earlier version of this protocol. This makes it more practicable and user friendly. At the end, the author provides a detailed analysis of the protocol.

Mobile banking actually is a system which facilitates financial services customer to conduct financial transaction via mobile phones or other electronic devices. Meanwhile, according to [7], mobile banking is a banking facility through mobile communication such as cellular phones with the provision of similar facilities with ATM but taking cash money.

According to Zainul Mufid, Rizal Bahaweres, Iwan Krisnadi [8], as well as development of mobile phone technology that

increases from WAP, GPRS and UMTS until HSPA for multimedia services to the next generation, banks are increasingly ready to provide services through the mobile phone. The bank will benefit more, cheaper admin fee, smaller number of branches, call centers are an efficient and economical maintenance costs. The following description of mobile banking system:

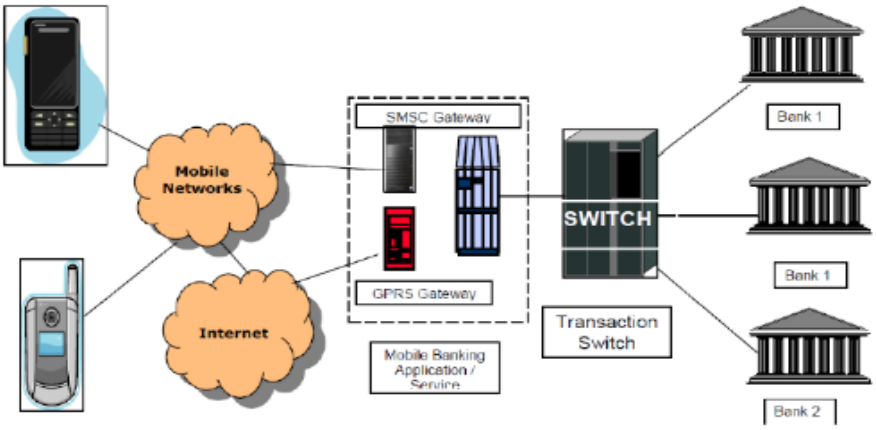

Figure 2. System mobile banking [9]

NFC is a short-range wireless connectivity technology-based standard that can make two-way simple and intuitive interaction between electronic devices. Communication between two NFC devices is done comfortably is by touching one another [10]. Meanwhile, according to Made Krisnanda [11], NFC is a short range wireless technology that can be used to exchange data between devices.

According to TeknoJurnal (2014), NFC technology has three modes, namely NFC card emulation mode, peer-to-peer mode, and reader/writer mode. The following NFC protocol chart:

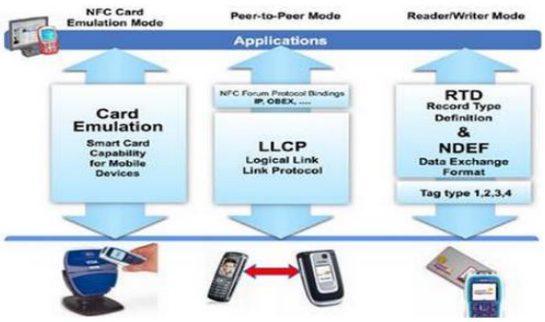

Figure 3. NFC Protocol

In America, the use of mobile payment is already very popular. NFC works such as PayPass MasterCard and MasterCard or credit cards. In San Francisco, NFC is used as a means of payment for parking. In the Austrian NFC is also used for the payment of a train ticket. Meanwhile quoted from (Detik, 2015), one of McDonald's fast food restaurants in the United States displaying a memo to employees that began on August 26, 2015, customers can use Android Pay to pay for food [12].

According to the JSON's official website, JSON is a lightweight data interchange format, easily read and written by human, and easily translated and made (generated) by computer. This format is based on part of the Programming Language JavaScript, Standard ECMA-262 3rd Edition - December 1999. JSON is a text format that is independent of the programming language whatsoever for using a style commonly used by programmers family C including C, C ++, C # , Java, JavaScript, Perl, Python etc. Because of these properties, making it ideal as a JSON- data exchange language.

According to the official website of JSON, JSON is made of two structures:

- A collection of name / value pairs. In some languages, this is expressed as an object, record, structure, dictionary, hash table, keyed list, or associative arrays.
- An ordered list of values. In most languages, this is expressed as an array, vector, lists, or sequences.

Broadly speaking, according to Gurpreet Singh [13], encryption is a technique to ensure the security of a data. Encryption algorithms make the process of substitution and transformation in plain text and convert it into

cipher text. Singh also specified that encryption algorithm is divided into two categories, namely symmetric-key and asymmetric-key. Symmetric key encryption is a cryptographic encryption and decryption using the same key. Meanwhile, encyprtion is asymmetric-key cryptography uses encryption and decryption keys are different, namely a public key and a private key.

Another research conducted by Azizah [14] stated that Advanced Encryption Standard (AES) is a form of encryption method used in the process of encoding a message. This algorithm began to be found in 1997, when the National Institute of Standards and Technology (NIST) made a contest to find a new algorithm that can replace DES.

Also according to [14], the encryption algorithm AES is a block cipher algorithm that uses the same key for encryption and decryption. The key that is used here is called a symmetric key. AES encryption operation using multiple rounds in the process of encoding the message. There are several methods use different keys in the encryption process AES. These methods are referred to as operating models. There are six kinds of operating models used in the process of AES encryption, the electronic code book (ECB), cipher block chaining (CBC), counter (CTR), cipher feedback (CFB), output feedback (OFB), Galois counter mode (GCM).

The input and output of the AES algorithm consists of a sequence of 128 bits of data. The sequence data that has been formed in a group of 128 bits is also referred to as a data block or plaintext will be encrypted into ciphertext. Cipher key of AES is composed of a key with a length of 128 bits, 192 bits or 256 bits. Differences key length will affect the number of rounds that will be implemented in this AES algorithm. Here is a table showing the number of round / rounds (Nr) which must be implemented on each of the key length [15].

The concept of mobile banking system development proposes by PT. Bank Panin Syariah Tbk using Near Field Communication (NFC) technology. Commonwealth Bank of Australia has been implementing NFC in mobile banking. The Mobile banking has a tap & pay feature, customer can make payment at location that accept MasterCard® PayPass™. Meanwhile, the author implements NFC technology in this application as client authentication and security system.

The development of mobile banking system with Android-based operating system in PT. Bank Panin Sharia Tbk is designed to be developed. Therefore, the author limites this writing among others:

1. The author uses Android Studio tools for application creation. Tools that author used in the manufacture of the NinjaMock mockup, while for application layout using Adobe Photoshop CS6. Tools that author used in making the system concept that Microsoft Visio 2010.
2. MySQL as database management. Mobile banking system consists of three databases on one server using hosting service in IdWebHost. Output data using JSON format.
3. Using smartphone Galaxy S4 with operating system Android Lollipop 5.1.1.
4. Using RAD system development method and system testing methods unit testing and user acceptance testing.
5. Process on mobile banking application, namely customer activation, call center, information balance, information transfer, information postpaid electricity bill, transfer transactions between fellow PT.Bank Panin Syariah Tbk, transfers between banks in Indonesia, favorite transaction, see location of ATM PT. Bank Panin Syariah Tbk, postpaid payment of electricity bills, and sign out.
6. Application is tested or only work on Android that have NFC support.

The purpose of this study was to develop a mobile banking application using NFC technology with Android-based operating system for PT. Bank Panin Syariah as client authentication and security system.

II. METHODS

Based on the data collection methods and development of systems that author use, the development phase for the application will use the Rapid Appilcation Development approach [16].

Rapid Application Development (RAD) is one method of developing an information system with a relatively short time. To develop a normal information system requires a minimum of 180 days but using the RAD method a system can be completed in only 30-90 days. The main goal of all system development methods is to provide a system that can meet the expectations of users, but often in developing a system does not involve the users of the system directly, so this causes the information system that is made far from the expectations of users that can result, although the system is acceptable but users are reluctant to use it or even users refuse to use it.

When RAD is implemented, users can become part of the overall system development process by acting as a decision maker at each stage of development.

RAD can produce a system quickly because the developed system can meet the wishes of the users so as to reduce the time for redevelopment after the implementation phase.

Testing perform using automation test requires fewer time and test cases to achieve coverage [17]

III. RESULT AND IMPLEMENTATION

3.1 Use Case Diagram

Use case diagrams mobile banking application can be seen on Figure 4.

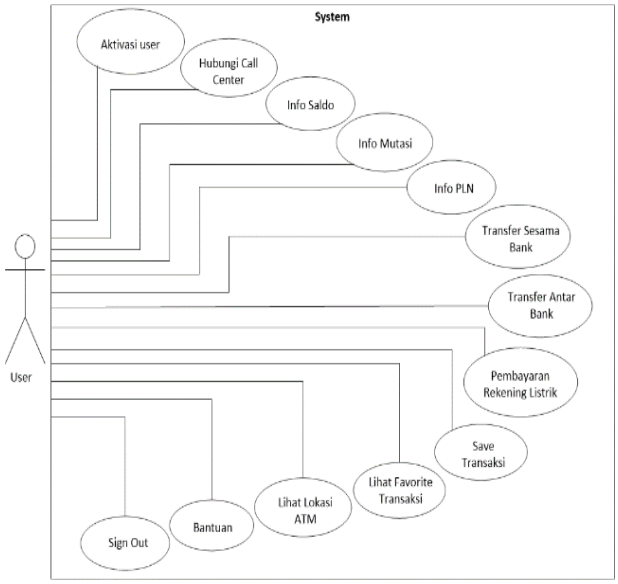

Figure 4. Use case diagram

3.2 NFC Source Code

Android Studio tools that I use has provided library NFC. Library used to be preceded by the word import. The picture below is an NFC library that author use in the development of mobile banking applications.

```
import android.nfc.FormatException;
import android.nfc.NdefMessage;
import android.nfc.NdefRecord;
import android.nfc.NfcAdapter;
import android.nfc.Tag;
import android.nfc.tech.MifareUltralight;
import android.nfc.tech.Ndef;
import android.nfc.tech.NfcA;
import android.nfc.tech.NfcF;
```

Figure 5. Source code library NFC

Authors create a class that contains model. Model that created in the class that is getType () and getValue (). Model getType () has the value of the type of the embedded NFC. Meanwhile, the model getValue () has a value messages stored on NFC card. Below is a drawing class that contains NFC models.

```
public static class TagInfo implements Parcelable {
    private String type;
    private String value;

    public TagInfo(String type, String value) {
        this.type = type;
        this.value = value;
    }

    public String getType() { return type; }

    public String getValue() { return value; }

    public static final Creator<TagInfo> CREATOR
            = new Creator<TagInfo>() {...};

    private TagInfo(Parcel in) {...}

    @Override
    public int describeContents() { return 0; }

    @Override
    public void writeToParcel(Parcel dest, int flags) {...}
}
```

Figure 6. Source code of NFC model

When user pressed NFC on smartphones, handleTagReceive method will be called from a class. Method handleTagReceive () will take the class parameter access. Method handleTagReceive () in charge of retrieving data from NFC card to be sent to class access it. Here is a picture of the source code handleTagReceive method ().

```
public static TagInfo handleTagReceive(Intent intent) {
    if (intent == null) {
        return null;
    }
    Tag tagFromIntent = intent.getParcelableExtra(NfcAdapter.EXTRA_TAG); // get tag from intent
    if (tagFromIntent == null) {
        return null;
    }

    Ndef tag = Ndef.get(tagFromIntent);  // get ndef object from tag
    try {
        tag.connect();
        NdefMessage ndefM = tag.getNdefMessage(); // get ndef message
        NdefRecord[] nrec = ndefM.getRecords(); // get nfc tag records (pages)

        StringBuilder sb = new StringBuilder();
        for (NdefRecord rec : nrec) {
            sb.append(new String(rec.getPayload())); // read record to string
        }
        return new TagInfo(tag.getType(), sb.toString());
    } catch (IOException e) {
        Log.e(TAG, "Unable to connect to NFC tag", e);
    } catch (FormatException e) {
        Log.e(TAG, "NFC tag has unknown format", e);
    }
    return null;
}
```

Figure 7. Source code method HandleTagReceive NFC

In the Figure 8, when application accesses the class activity will automatically call directly method onResume (). Method onResume () will check NFC technology on smartphones. Smartphones that have the NFC technology will continue to carry that class when the user pressed the NFC.

```
@Override
protected void onResume() {
    super.onResume();
    if (this.getPackageManager().hasSystemFeature(
            PackageManager.FEATURE_NFC)) {
        this.nfcAdapter.enableForegroundDispatch(this,
                this.getPendingIntent(), this.getIntentFilters(),
                Nfc.techList);
    }
}
```

Figure 8. Source code method OnResume NFC

In the Figure 9, the method OnNewIntent() will be executed when the user pressed the NFC card in smartphone. Method OnNewIntent() will call the method handleTagReceive() to get the detail NFC. If the feedback from the NFC is not empty, then the application will call a method sendReturnMessage(). Method sendReturnMessage() contains the command took the NFC detail using a model that has been previously declared. The NFC models namely getType and getValue of NFC taped by the user.

```
@Override
protected void onNewIntent(Intent intent) {
    super.onNewIntent(intent);
    System.out.println("new intent");
    Nfc.TagInfo info = Nfc.handleTagReceive(intent);
    if (info != null) {
        this.sendReturnMessage(Activity.RESULT_OK, info);
    }
}


public void sendReturnMessage(int status, Nfc.TagInfo info) {
    // if nfc is present setup nfc adapter
    Nfc.TagInfo infos = info;
    nilai_nfc = String.valueOf(infos.getValue());
    if (!nilai_nfc.equals("")) {
        ll_nfc.setVisibility(View.GONE);
        ll_pin.setVisibility(View.VISIBLE);
        st_no_kartu = nilai_nfc.substring(3);
        System.out.println("nfc data card : " + nilai_nfc);
        System.out.println("nfc data: " + st_no_kartu);
        System.out.println("nfc data: " + String.valueOf(infos.getType()));
    }
}
```

Figure 9. Source Code Method OnNewIntent NFC

On this approach, the application developed using technology one transaction password, soft token, or hard token that enable customers who do not use smart phones with NFC technology can make mobile banking transaction.

IV. CONCLUSION

Based on research results and writing that author explains, it can be concluded that the mobile banking system PT. Bank Panin Syariah Tbk implement Near Field Communication

technology, PIN, and AES encryption as a way to provide security. Development of mobile banking system PT. Bank Panin Syariah Tbk starting from collection of data and information, identification system, designing 12 Use Case Diagram, Activity Diagram 9, 12 Sequence Diagram, Class Diagram 3 design, database design, user interface design, code generation program, and testing using the programming language Java with Android Studio tools, programming languages PHP, MySQL database, hosting IdWebHost using JSON services, RAD system development methods, and testing methods with unit testing and user acceptance testing.

The author realized that in doing research still has shortcomings. Therefore, the author advised to develop the study, among other:

1. The existence of call center feature at Central Office in addition to the Jakarta area.
2. Using near field communication reader technology. The Implementation is expected that mobile banking can be used to make purchases in stores at Indonesian Area.

REFERENCES

[1] "Riset Kadence: Layanan Banking E-Channel di Mata Nasabah - Tribunnews.com." [Online]. Available: https://www.tribunnews.com/bisnis/2014/03/06/riset-kadence-layanan-banking-e-channel-di-mata-nasabah. [Accessed: 27-May-2020].

[2] "Pengguna Mobile Banking Lebih Banyak Ketimbang Kartu Kredit - SHARINGVISION." [Online]. Available: https://sharingvision.com/pengguna-mobile-banking-lebih-banyak-ketimbang-kartu-kredit/. [Accessed: 27-May-2020].

[3] "Mobile banking to grow to 2B users by 2020: report | Retail Dive." [Online]. Available: https://www.retaildive.com/ex/mobilecommercedaily/mobile-banking-to-grow-to-two-billion-users-by-2020-report. [Accessed: 27-May-2020].

[4] "(PDF) Development of an android document management." [Online]. Available: https://www.researchgate.net/publication/337872293_Development_of_an_android_document_management/figures?lo=1. [Accessed: 27-May-2020].

[5] N. El Madhoun and G. Pujolle, "Security enhancements in EMV protocol for NFC mobile payment," in *Proceedings - 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 10th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Symposium on Parallel and Distributed Proce*, 2016.

[6] P. Pourghomi, M. Qasim, and G. Ghinea, "A Secure Cloud-Based NFC Mobile Payment Protocol," *Int. J. Adv. Comput. Sci. Appl.*, 2014.

[7] A. A. Shaikh and H. Karjaluoto, "Mobile banking adoption: A literature review," *Telematics and Informatics*. 2015.

[8] "Analisis Perencanaan Bisnis Perusahaan Penyedia Jasa Switching dan Aplikasi Mobile Banking Bank X | Mufid | InComTech: Jurnal Telekomunikasi dan Komputer." [Online]. Available: https://publikasi.mercubuana.ac.id/index.php/Incomtech/article/view/1108/807. [Accessed: 27-May-2020].

[9] sanjeev banzal, "Mobile Banking and M-Commerce and Related Issues," 2008.

[10] G. Madlmayr, C. Kantner, and T. Grechenig, "Near field communication," in *Secure Smart Embedded Devices, Platforms and Applications*, 2014.

[11] M. Krisnanda, "3. Penggunaan Teknologi Near Field Communication Pada Telepon Seluler Untuk Micro Payment dan Loyalty Management," *J. Inform.*, vol. 7, no. 1, Mar. 2015.

[12] "McDonald's preparing for launch of NFC-based mobile payments system | Retail Dive." [Online]. Available: https://www.retaildive.com/ex/mobilecommercedaily/mcdonalds-preparing-for-launch-of-mobile-payment-system-memo-shows. [Accessed: 27-May-2020].

[13] G. Singh, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," 2013.

[14] "Implementasi Fungsi Kriptografi dan Otentikasi Sidik Jari Pada Pemungutan Suara Berbasis Elektronik (E-voting) - PDF Free Download." [Online].

Available: https://docplayer.info/35256444-Implementasi-fungsi-kriptografi-dan-otentikasi-sidik-jari-pada-pemungutan-suara-berbasis-elektronik-e-voting.html. [Accessed: 27-May-2020].

[15] S. Heron, "Advanced Encryption Standard (AES)," *Netw. Secur.*, 2009.

[16] W. S. Davis, D. C. Yen, D. C. Yen, and W. S. Davis, "Rapid application development (RAD)," in *The Information System Consultant's Handbook*, 2020.

[17] R. B. Bahaweres, K. Zawawi, D. Khairani, and N. Hakiem, "Analysis of statement branch and loop coverage in software testing with genetic algorithm," in *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 2017, vol. 2017-December.

Copyright

All unpublished manuscripts can be submitted elsewhere. The author is responsible for the publication's permission or recognition of images, tables and numbers in the manuscript he sent. The manuscript is not a result of plagiarism and does not violate any other rights of third parties. The author agrees that the decision to publish or not to publish a manuscript in the journal submitted by the author, is entirely the right of the journal manager. Prior to the final acceptance of the manuscript, the author is required to assert in writing, that the written post is copyright of the author and assign this copyright to the journal manager.