Design and Build Zakat Website Application Based on QR Code Using Cipher Block Chaining Algorithm

Tito Sugiharto*, Agus Yadi Ismail, Heri Herwanto, Daswa, M Irwansyah Somantri, Andrey Andriansyah, Novandra Maulana

Universitas Kuningan, Kuningan, Indonesia

{tito@uniku.ac.id}

Abstract. Zakat is a certain part of the property that must be issued by every Muslim if it has reached the specified conditions. As one of the pillars of Islam, Zakat is paid to be given to those who are entitled to receive it. Zakat is managed by an official body established by the government, namely the National Amil Zakat Agency (BAZNAS). BAZNAS was formed by the government based on the Decree of the President of the Republic of Indonesia No. 8 of 2001 which has the task and function of collecting zakat, infaq and alms at the national level. BAZNAS has an extensive network spread across 34 provinces and in 463 regencies and cities throughout Indonesia. BAZNAS Majalengka is one part of the central BAZNAS network that is always committed to managing and collecting zakat, infaq and alms from the community. BAZNAS Majalengka in the process of collecting zakat, infaq and alms is still using the direct transaction method. The direct transaction method has several problems including the giver and recipient of zakat must meet in person, the recording process must be carried out in detail, limited distance and time, and the recording process has not been digitally computerized. A website-based application is needed that can make it easier for everyone to make zakat transactions to BAZNAS Majalengka. With this application, it is expected to increase zakat income to BAZNAS Majalengka and can facilitate zakat giving transactions. This application is designed using the Rational Unified Process (RUP) system development method. The RUP method consists of four stages, namely: Inception, Ellaboration, Construction, and Transition. In the transaction process for giving zakat, a QR Code is used by applying the Cipher Block Chaining algorithm. The result of this research is a website application for giving zakat.

Keywords: Zakat; QR Code; Ciper Block Chaining; Baznas; RUP

1 Introduction

BAZNAS Majalengka is one part of the central BAZNAS network that is always committed to managing and collecting zakat, infaq and alms from the community. BAZNAS Majalengka in the process of collecting zakat, infaq and alms is still using the direct transaction method. The direct transaction method has several problems including the giver and recipient of zakat having to meet in person, the recording process must be done in detail, limited in distance and time, and the recording process has not been digitally computerized. A website-based application is needed that can make it easier for everyone to make zakat transactions to BAZNAS Majalengka. With this application, it is expected to increase zakat income to BAZNAS Majalengka and can facilitate zakat giving transactions.

UNISET 2021, December 02, Kuningan, Indonesia

DOI 10.4108/eai.2-12-2021.2320297

To facilitate the transaction process for giving zakat through the website media, transaction facilities using a QR-Code are needed. QR Codes are used to encode and decode data at a rapid rate. Using camera phones to read two dimensional barcodes for various purposes is currently a popular topic in both research and in practical applications. But until now, the information provided by QR Codes was solely static[1]. Quick response (QR) codes are barcodes comprising white and black blocks, which have been widely adopted in mobile applications such as communication, payment, etc, with the pervasive built- in cameras on smartphones[2].

Many researches on the use of QR Codes have been carried out including by Fong with the title

Smart City Bus Application with Quick Response (QR) Code Payment. the results of his research represent the results of a system and acceptance Smart City Bus Application testing, Android application specifically providing access to public bus transportation information such as display bus route, bus live location, login bus notification, bus fare calculation and payment using QR code[3]. In addition, pradipta de also conducted research on QR codes with the title An Assessment of QR Code as a User Interface Enabler for Mobile Payment Apps on Smartphones with research results with 48 users to identify the answer to two different questions: (a) how do users with text-based UIs that are more familiar with the new QR code-based UIs perform? (b) not lacking experience with smartphone use acts as an entry barrier for apps designed for smartphones? Users show a significant improvement in completing tasks for the same task when using QR Code based UI versus text based UI on smartphones. User response under various smartphone experience is not affected when using QR code based applications[4].

In this study, our goal is to build a QR Code-based zakat web application using the Cipher Block Chaining algorithm that can facilitate zakat giving transactions. The Cipher Block Chaining (CBC) algorithm is the application of a feedback mechanism to a block of bits where the results of the previous block encryption are fed back into the current block encryption processs. The trick, the current plaintext block is XORed first with the previously encrypted ciphertext block, then the XOR results are entered into the encryption function. With the CBC algorithm, each ciphertext block depends not only on its plaintext block but also on all previous plaintext blocks[5].

2 Methodology

In this paper used a methodology consisting of three methods, namely data collection methods,system development methods and problem solving methods. Data collection methods are methods or techniques that can be used by researchers to collect data. The data collection method in this study used the observation method, interview method, and literature study method.

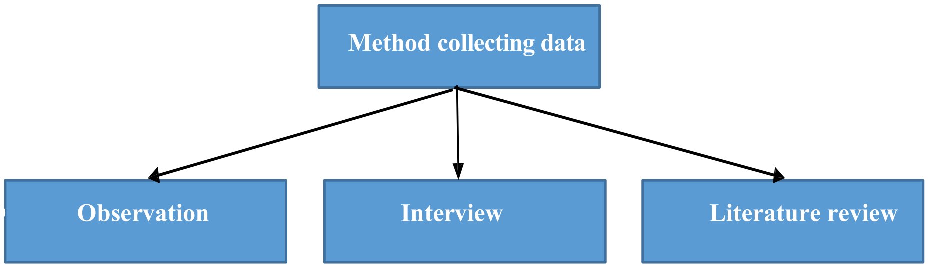


Figure 1. Method of collecting data

The observation method was carried out by direct observation to the research location at BAZNAS Majalengka to find out the activities and workflow that took place. In the observation method obtained data related to the process of zakat management activities that have not used a website-based application. The interview method is a data collection method used to obtain information directly from the source. Interview activities were carried out with the leadership of BAZNAS Majalengka in order to explore information and problems. The literature study method is a data collection technique by collecting relevant information and obtained from books or journals that are related to BAZNAS, QR Code and encryption and decryption s ystems on the Cipher Block Chaining algorithm.

The system development method used in this paper uses the Rational Unified Process (RUP) method. Rational Unified Process is a software engineering method developed by collecting various best practices in the software development industry[6]. The RUP model is very good for the Unified Modeling Language (UML)-based software development process. This is because the RUP method uses

Object Oriented Programming (OOP) methods in dividing step by step and iterating between the components involved.

The activities carried out in the RUP methodology are creating and maintaining models. The RUPalso includes a discussion of the UML implementation. So that we can distinguish RUP is a process or stage that is done in software engineering, while UML is a standard language used to describe, describe, build, and document the devices used in building software[7].

The RUP method consists of four stages, namely Inception, Ellaboration, Construction, and Transition. The following is an explanation of the system development using the Rational Unified Process (RUP) Method:

a. Inception

   This stage is the earliest stage where the evaluation activity of a software project is carried out. In this case, we collected data by direct observation to the research site, namely BAZNAS Majalengka. We collect data needed to support application development, such as conducting interviews related to the menu ordering system and payment processing with the leadership of BAZNAS Majalengka. We also conducted literature studies related to the Cipher Block Chaining algorithm, QR Code, android application programming, and web application programming with PHP. The data that has been collected is then analyzed to determine user needs and the design of the system to be made.

b. Elaboration

   The purpose of this stage is to get an overview of the needs, requirements and main functions of the software. In this case the author focuses on planning the system architecture. Activities carried out at this stage include making subsystem architecture design (architecture pattern), display component design, modeling with UML (Unified Modeling Language) diagrams and making documentation.

c. Construction

The steps carried out in this phase are:

- Implementation

  At this stage the author begins to write program code (coding) using the Android programming language for users and PHP for admin
- Testing

  At this stage, the system is tested, the author uses blackbox, whitebox and User Acceptance Testing (UAT) testing.

d. Transition

This stage is focused on how to deliver the finished software to the user. In this case, the author willinstall the system so that it can be understood by the user. Activities at this stage include user training and maintenance.

The problem solving method used in this QR code is using the Cipher Block Chaining method. Cipher Block Chaining is one of the developments of the Block cipher algorithm, this algorithm will divide the clear text that will be sent with a certain size (called a block) with the bit length of each block in accordance with the length of the bit in the key, and each block is encrypted using the same key. and XOR it with the result of the previous block encryption[8].

Cipher Block Chaining works in block mode, which is grouping plaintext binaries into several groups according to the conditions set by the user (the person who encrypts the message). The encryption and decryption process is carried out by XORing each block value with the previous block then the result obtained from the XOR operation in XOR it returns with the key. Binary result of XOR operation on each block will be shifted to the left or right by the amount specified by the user system. The initial value and key are set before the encryption or decryption process is carried out and must be agreed upon by the encrypter and the decryptor. Key length and initial value (initial vector/C0) must be equal to the number of bits per group[9].

Steps in completing the Cipher Block Chaining algorithm process (CBC) are as follows:

1. Input plaintext or ciphertext, then convert the decimal value to binary
2. Determine the value of the number of bits for each group, key, initialization vector (C0)
3. Group the plaintext and ciphertext binaries into blocks according to the number of bits per group that has been previously determined.
4. Perform the encryption or decryption process on each block/binary group of plaintext or ciphertext where each block is interdependent with other blocks.
5. Perform the process of shifting the plaintext and ciphertext bits according to the number of bits set by the user, the result of this shift is the final result of the encryption or decryption process.

The flowchart of the encryption and decryption of the Cipher Block Chaining algorithm can be seen in the following figure 2.

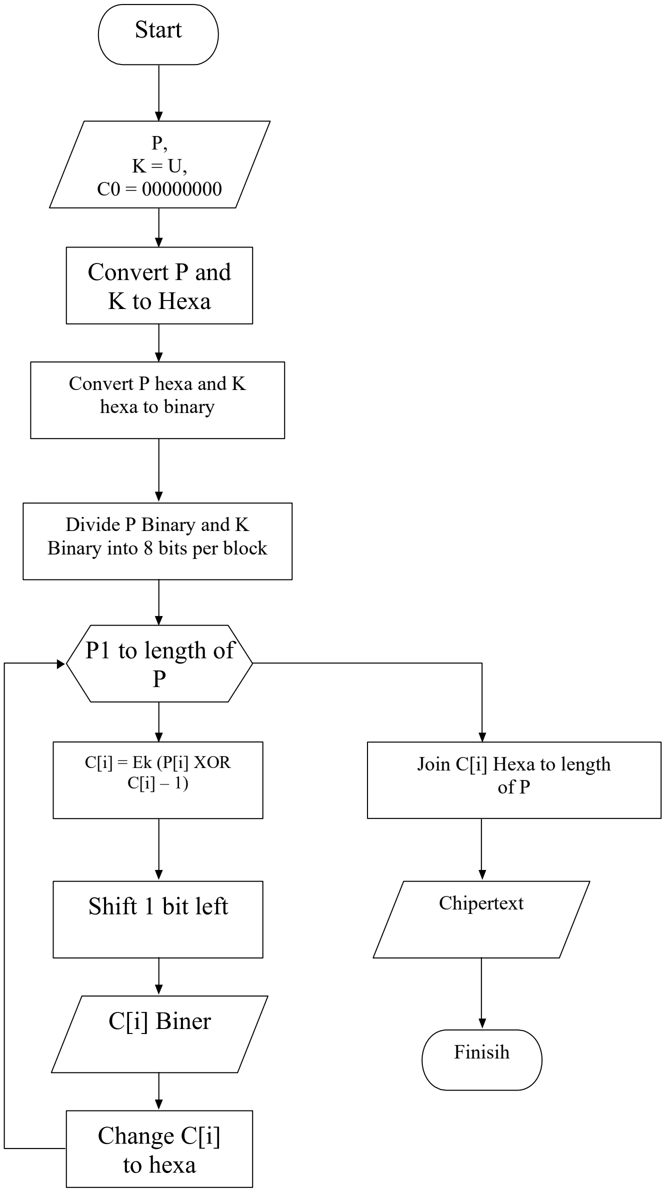

Start
P,
K = U,
C0 = 00000000
Convert P and K to Hexa
Convert P hexa and K hexa to binary
Divide P Binary and K Binary into 8 bits per block
P1 to length of P
C[i] = Ek (P[i] XOR C[i] – 1)
Shift 1 bit left
C[i] Biner
Change C[i] to hexa
Join C[i] Hexa to length of P
Chipertext
Finisih

Figure 2. Flowchart Encryption Cipher Block Chaining

Mathematically, encryption and decryption with the Cipher Block Chaining algorithm is stated as follows:

Ci = Oak (Pi Ci – 1) Pi = Dk(Ci Ci – 1)

3 Result and Discussion

The results of this journal produce a use case diagram design for the zakat website application using a QR code as shown in Figure 3.

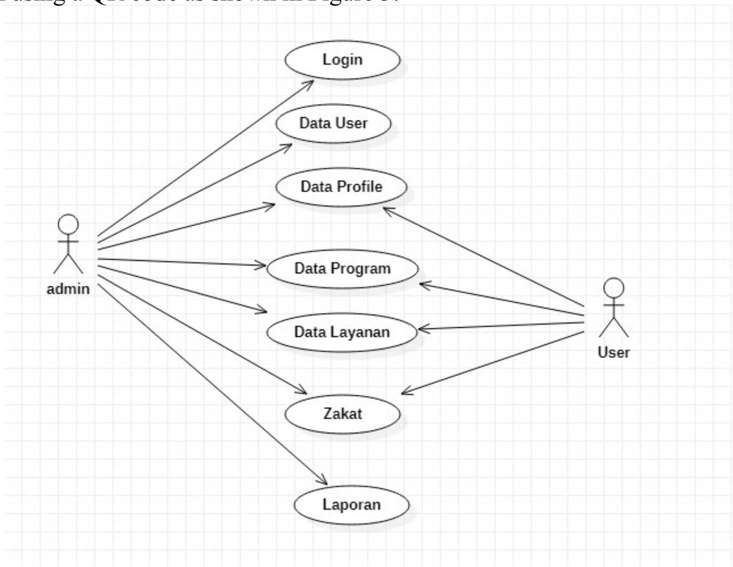
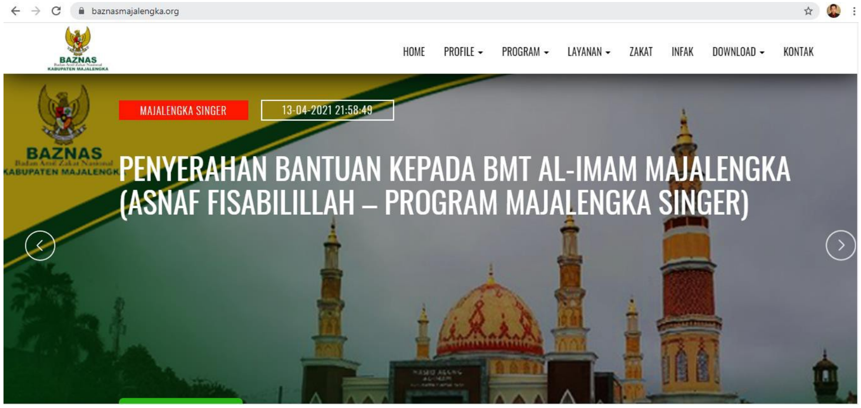


Figure 3. Uce Case Diagram

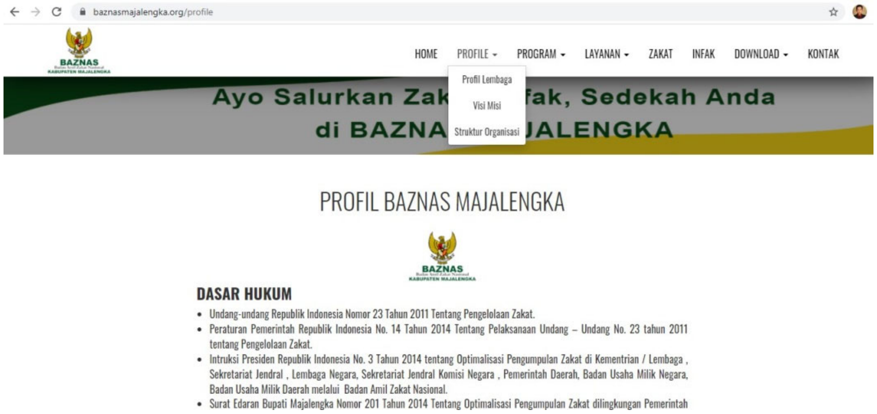
The following is the result of the display of the zakat website application. The main menu page is the first page display when the website is opened. in the main menu page display there are several menus including the home menu, profile, program, service, zakat, infaq, downlaod, contact. Figure 4 is a display of the main menu page.



PENYERAHAN BANTUAN KEPADA BMT AL-IMAM MAJALENGKA (ASNAF FISABILILLAH – PROGRAM MAJALENGKA SINGER)

Figure 4. Main Menu Page

The profile menu page contains three sub menus, namely: institution profile, vision and mission, and organizational structure. Figure 5 is a display of the profile page menu.



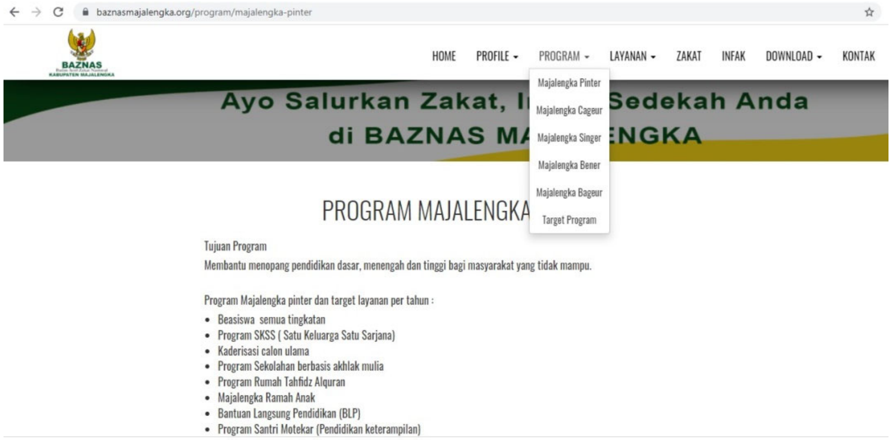
PROFIL BAZNAS MAJALENGKA

DASAR HUKUM

- Undang-undang Republik Indonesia Nomor 23 Tahun 2011 Tentang Pengelolaan Zakat.
- Peraturan Pemerintah Republik Indonesia No. 14 Tahun 2014 Tentang Pelaksanaan Undang – Undang No. 23 tahun 2011 tentang Pengelolaan Zakat.
- Intruksi Presiden Republik Indonesia No. 3 Tahun 2014 tentang Optimalisasi Pengumpulan Zakat di Kementrian / Lembaga , Sekretariat Jendral , Lembaga Negara, Sekretariat Jendral Komisi Negara , Pemerintah Daerah, Badan Usaha Milik Negara, Badan Usaha Milik Daerah melalui Badan Amil Zakat Nasional.
- Surat Edaran Bupati Majalengka Nomor 201 Tahun 2014 Tentang Optimalisasi Pengumpulan Zakat dilingkungan Pemerintah

Figure 5. Profile Page Menu

The program menu page contains six menus, namely: Majalengka Pinter, Majalengka Bageur, Majalengka Cageur, Majalengka Singer, Majalengka Bener, Target Program. Figure 6 is a display of the program menu page.



PROGRAM MAJALENGKA

Tujuan Program

Membantu menopang pendidikan dasar, menengah dan tinggi bagi masyarakat yang tidak mampu.

Program Majalengka pinter dan target layanan per tahun :

- Beasiswa semua tingkatan
- Program SKSS (Satu Keluarga Satu Sarjana)
- Kaderisasi calon ulama
- Program Sekolahan berbasis akhlak mulia
- Program Rumah Tahfidz Alquran
- Majalengka Ramah Anak
- Bantuan Langsung Pendidikan (BLP)
- Program Santri Motekar (Pendidikan keterampilan)

Figure 6. Program Page Menu

The service menu page contains five sub menus including donations, online alms, calculating zakat, account numbers, infaq. Figure 7 is an illustration for the service page menu. On this page there is also a section that contains a QR code for processing alms giving transactions

QRIS GPN

BAZNAS KAB MAJALENGKA

Klik aplikasi · Scan · Masukan Nominal · Selesai

Mari tunaikan

Zakat, Infak, Shadaqah

lebih mudah dan nyaman melalui QRIS.

Caranya :

1. Buka aplikasi pembayaran digital
2. Klik tombol scan / pay / bayar
3. Scan QRIS ini
4. Masukan nominal zakat
5. Lanjutkan pembayaran

Scan QR dengan

BCA mobile · OVO · ShopeePay · gopay · DANA · Link Aja!

BAZNAS
Badan Amil Zakat Nasional
KABUPATEN MAJALENGKA

0811-223-9494 · www.baznasmajalengka.org

Figure 7. QR Code

4 Conclusion

The conclusions that can be drawn after conducting this research are as follows:

1. This research produces a zakat web application using the Qr Code as one of the methods for transactions.
2. In this study, we succeeded in implementing the Cipher Block Chaining Algorithm which was generated in the form of a Qr Code for the encryption and decryption of transaction id.
3. This application can help in the process of giving zakat quickly, easily, and safely
4. This application can make it easier for BAZNAS Majalengka in managing incoming zakat or donations because it is already computerized with the system

References

[1] Rouillard, J. (2008). Contextual QR codes. Proceedings of ICCGI 2008: The 3rd International Multiconference on Computing in the Global Information Technology.

[2] Li, Y., Chen, Y.-C., Ji, X., Pan, H., Yang, L., Xue, G., & Yu, J. (2020). Toward a secure QR code system by fingerprinting screens. 1–3. https://doi.org/10.1145/3372224.3418165

[3] Fong, S. L., Yung, D. C. W., Ahmed, F. Y. H., & Jamal, A. (2019). System testing. Navigation: Science and Technology, 329–388. https://doi.org/10.1007/978-981-10-8791-2_11

[4] Sudaryono. (2015). Metode Riset di Bidang TI:Penerbit Andi. Yogyakarta

[5] Andriani, D. (2017). Perancangan Aplikasi Penyandian Teks Dengan Menggunakan Algoritma Chiper Block Chaining. Jurnal Teknik Informatika Unika St. Thomas (JTIUST), 02(338), 14–23.

[6] A.S Rosa, Salahuddin, M (2011), Modul Pembelajaran Rekayasa Perangkat Lunak(Terstruktur dan Berorientasi Objek).

[7] Pressman, Roger S. 2010. Rekayasa Perangkat Lunak. Yogyakarta: Andi.

[8] Zebua, T. 2015. "PENGAMANAN DATA TEKS DENGAN KOMBINASI CIPHER BLOCK CHAINING DAN LSB-1". Seminar Nasional Inovasi dan Teknologi Informasi 2015.

[9] Dewi Rosmala (2012), Implementasi Mode Cipher Block Chaining (CBC) pada pengamana Data, Vol.3, 2012