ITDM: Information Technology Development And Management
Volume 2, (2) 2026, p. 67-78
E-ISSN: XXXX-XXXX
©2026. The Author(s). This is an open acces article under cc-by-sa

Employee Data Security Using the Advance Encryption Standard Algorithm in Employee Data Applications (Case Study: Finance Section of the Lebak District Ministry of Religious Affairs Office)

Hendra Bayu Suseno [1]*, Rizqi Laeli [2], Victor Amrizal[3], Feri Fahrianto[4], Andrew Fiade[5], Mohammad Liyananta Septipalan[6]

[1,2,3,4,5] Department of Informatics Engineering, UIN Syarif Hidayatullah Jakarta, Indonesia
[6] Department of Master Information Technology, UIN Syarif Hidayatullah Jakarta, Indonesia

[1]* hendra.bayu@uinjkt.ac.id
[2]rizqi.laeli21@mhs.uinjkt.ac.id
[3]victor.amrizal@uinjkt.ac.id
[4]feri.fahrianto@uinjkt.ac.id
[5]andrew.fiade@uinjkt.ac.id
[6]mohammad.liyananta24@mhs.uinjkt.ac.id

Received: 8 July 2026, Revised: 9 July 2026, Accepted: 13 July 2026, Published: 31 October 2026

Abstract

The Ministry of Religious Affairs of Lebak Regency is a government agency responsible for religious affairs in the Lebak Regency, Banten. In the Finance Section, employee data management is still done manually using Excel files, which poses a risk of delays in payroll processing and is vulnerable to data loss or misuse. To address these issues, this study developed a web-based employee data management application incorporating the Advanced Encryption Standard (AES) 128-bit Cipher Block Chaining (CBC) algorithm to protect sensitive data such as National Identity Numbers (NIK), addresses, and phone numbers. Using the Rational Unified Process (RUP) development method, which consists of four stages—inception, elaboration, construction, and transition—this application can help streamline the employee data management process in a more structured manner. User Acceptance Testing (UAT) results showed a user satisfaction rate of 93.2%, and the implementation of AES in this application is used to enhance employee data protection.

Keywords: AES 128-bit, CBC, Data Security, RUP.

I. Introduction

The Ministry of Religious Affairs of Lebak Regency is a government agency responsible for religious affairs in the Lebak Regency, Banten. This agency manages various services such as religious affairs, Hajj and Umrah, zakat and waqf, as well as other religious guidance. With the increasing diversity of services managed, employees are required to actively keep up with the rapid development of technology. This is no exception in the Finance Section. Observations and interviews conducted with Mr. Fadli Kurnia Dwi Cahyono as the Commitment Making Officer (CMO) on June 26, 2025, revealed that although the agency has a central system for managing employee data, the system does not fully support the operational needs of the Finance Section. One of the main challenges is the lack of direct access to complete employee data, resulting in data storage still being done manually using Excel files. This situation forces finance staff to first request data from the human resources department before they can create pay slips.

ITDM: Information Technology Development And Management
Volume 2, (2) 2026, p. 67-78
E-ISSN: XXXX-XXXX
©2026. The Author(s). This is an open acces article under cc-by-sa

This issue highlights the need for an integrated employee data management application to support the smooth administration of the Finance Section at the Ministry of Religion in Lebak District. The application is designed as a website to be accessible via computers or smartphones, making it easier for staff to manage employee data and generate pay slips. However, data digitization also introduces new risks, including the potential for data leaks, theft, or loss if not accompanied by adequate security systems. Data breaches in the digital age are not new, with major incidents occurring in both government institutions and private companies. For example, the data breach at the General Elections Commission (KPU) involving National Identification Numbers (NIK) and voter personal data [1], the data breach at the Health Social Security Agency (BPJS Kesehatan) affecting 279 million people [2], and the incident in the e-commerce sector where 91 million user accounts were sold [3]. These cases underscore the need for special protection in managing sensitive data to minimize the risk of leaks.

Various data security strategies have been studied, ranging from input validation to prevent SQL injection, the implementation of Role-Based Access Control (RBAC) to address misuse of access rights, the use of Intrusion Detection Systems (IDS) to minimize the impact of malware, to the implementation of encryption to maintain the confidentiality of information [4]. Among these strategies, encryption is one of the most effective techniques because it can convert original data (plaintext) into ciphertext that cannot be read without a decryption key [5]. Previous research has also shown that the application of cryptographic algorithms can prevent the leakage of confidential data [6]. This is particularly relevant given that personal data such as names, addresses, email addresses, phone numbers, and national identification numbers are often the primary targets of cyberattacks [7].

Among various cryptographic algorithms, the Advanced Encryption Standard (AES) is widely used due to its advantages in processing speed and high security levels [8]. Research [9] shows that AES is faster in encryption and decryption processes compared to the Twofish algorithm. This is also confirmed by [10], which found that AES-128 has a shorter processing time than Twofish or Blowfish. Additionally, AES supports key lengths of 128, 192, and 256 bits, enhancing data security layers [11]. In its implementation, the Cipher Block Chaining (CBC) mode was chosen because it can scramble each data block using an XOR operation with the previous block plus an Initialization Vector (IV), so that the original data pattern is not visible. Testing by [12] proved that this mode has an average encryption speed of 14.2 ms and decryption speed of 13.2 ms.

In addition to security aspects, the success of application development is also greatly influenced by the appropriate software development method. The Rational Unified Process (RUP) was chosen for its iterative and flexible nature, making it applicable to projects of various scales [13]. This method consists of four main phases: inception, elaboration, construction, and transition, ensuring that system development proceeds in a structured manner and aligns with user needs.

Based on these issues, this study focuses on developing a web-based employee data management application for the Finance Section of the Ministry of Religious Affairs in Lebak Regency, with the application of the Advanced Encryption Standard (AES) Cipher Block Chaining (CBC) algorithm to maintain the security of sensitive data. This research aims to produce an application that not only supports financial administration processes, particularly the creation of pay slips, but also provides protection for employee data from the risk of leakage or misuse. In addition, the results of this research are expected to provide academic benefits for the development of literature in the field of data security, as well as practical benefits for government agencies and other organizations facing similar challenges in employee data management.

ITDM: Information Technology Development And Management
Volume 2, (2) 2026, p. 67-78
E-ISSN: XXXX-XXXX
©2026. The Author(s). This is an open acces article under cc-by-sa

II. Related Work

Data security has become an important issue in information systems, particularly in applications that manage sensitive employee and financial information [14]. Previous studies have investigated various approaches to protect sensitive data, including access control, database security, and cryptographic techniques. Tanjung and Nasution [5] reviewed several database security strategies and emphasized that data protection should involve multiple mechanisms, including input validation, access control, intrusion detection, and encryption. Among these approaches, encryption provides an additional layer of protection by transforming plaintext into ciphertext, thereby reducing the risk of unauthorized access to sensitive information. Several studies have specifically investigated the application of cryptographic algorithms for protecting organizational data. Syahputra et al. [6] implemented the Vigenere Cipher to secure payroll data. Their study demonstrated that cryptographic techniques can be applied to protect sensitive payroll information. However, the use of classical cryptographic algorithms may provide different levels of security and computational performance compared with modern symmetric encryption standards. This consideration is important for employee information systems because the managed data may include personally identifiable information and financial information.

The Advanced Encryption Standard (AES) has been widely studied as an alternative for securing sensitive data because of its security and computational efficiency. Awal et al. [9] compared the encryption and decryption performance of Rijndael and Twofish and demonstrated the applicability of AES-based encryption for data protection. Similarly, Assa-Agyei and Olajide [10] conducted a comparative study of AES, Twofish, and Blowfish for secure data transmission and reported differences in encryption performance among the algorithms. These studies indicate that AES provides a suitable balance between security and processing efficiency for information systems that require data confidentiality.

The selection of AES operating mode is also an important consideration in practical implementation. Nugrahantoro et al. [11] investigated the use of AES with Cipher Block Chaining (CBC) mode for information security. CBC processes data blocks sequentially by combining each plaintext block with the previous ciphertext block through an XOR operation and uses an Initialization Vector (IV) to introduce variability into the encryption process. This approach can reduce recognizable patterns in encrypted data. Therefore, AES-128-CBC is considered relevant for applications that store sensitive information in databases.

In addition to data security, the software development methodology influences the effectiveness of information system implementation. Chandra et al. [13] applied the Rational Unified Process (RUP) to develop a web-based promotion and sales application. RUP provides an iterative development framework consisting of inception, elaboration, construction, and transition phases. The approach allows system requirements, architecture, implementation, and deployment to be developed systematically. In the context of employee information systems, the iterative characteristics of RUP are useful for aligning system functionality with the operational requirements of users.

Although previous studies have examined cryptographic techniques for securing organizational data and the implementation of RUP for web-based information systems, there is still limited integration of these approaches in employee data management systems within government financial units. Existing studies tend to focus either on the comparison of encryption algorithms, protection of specific datasets such as payroll information, or software development without explicitly integrating database-level encryption into the developed application. Therefore, this study proposes a web-based employee data management application for the Finance Section of the Ministry of Religious Affairs of Lebak Regency by integrating AES-128 with CBC mode to protect sensitive employee information, including national identification numbers, addresses, telephone numbers, and salary-related data. The system is developed using RUP and evaluated through Black Box Testing and User Acceptance Testing (UAT). This integration is expected to provide both functional support for employee and payroll administration and an additional layer of protection for sensitive employee data.

ITDM: Information Technology Development And Management
Volume 2, (2) 2026, p. 67-78
E-ISSN: XXXX-XXXX
©2026. The Author(s). This is an open acces article under cc-by-sa

III. Research Methodology

In this research, the author used the Rational Unified Process method. This method employs an iterative approach, dividing development into several iterations. Each iteration covers a significant portion of the development phase and builds on the results of the previous iteration. This approach allows for gradual improvements until the final product is complete. The stages in the Rational Unified Process (RUP) method are as follows [15]:

A. Inception

This stage describes a general overview of the Finance Section of the Ministry of Religious Affairs Office of Lebak Regency, identifies problems, and determines the system to be developed through the analysis process. In the analysis stage, the author understands the system requirements by collecting data from several sources. The steps to be taken in system development include (1) Business Modeling, where the author analyzes the business processes and current systems in the Finance Section of the Ministry of Religious Affairs Office of Lebak Regency based on the results of observations and interviews. The analysis includes workflows, information needs, and employee data management problems. The results of the analysis are then modeled using the Business Process Model and Notation (BPMN) as the basis for identifying the needs of the system to be developed. Next, (2) Requirements, where the author defines system requirements based on the results of the analysis of the current business processes that have been modeled previously. This stage aims to formulate the specifications of the proposed system requirements that are expected to be able to answer the problems in the Finance Section of the Ministry of Religious Affairs Office of Lebak Regency. This needs identification includes functional and non-functional needs which will later become the basis for system design in the next stage.

B. Elaboration

This stage is the process of compiling a comprehensive system design based on the results of the analysis conducted in the inception phase. At this stage, the author translates the previously identified needs and specifications into system design and database design. The design produced at this stage will be the main reference in the system development and implementation stages. The steps in this stage are: (1) creating a use case diagram used to describe the interaction between users (actors) and the system. This diagram can help understand the main features that will be developed in the application, (2) an activity diagram used to model the workflow in the application, describing the activities of each process. This diagram can help in understanding how data is processed in the application, (3) a sequence diagram used to describe the interaction between objects in a certain time sequence. This diagram can also help in understanding how communication between system components takes place.

C. Construction

This stage is the phase in which the results of the analysis and design are implemented and tested. In the construction phase, the previously created design is implemented into a real system. The author begins building system components according to the design specifications, including program code, as well as integration with the database. After implementation is complete, testing is carried out to ensure that the system functions correctly and meets the established needs. This testing includes functional, performance, and security tests to ensure the quality and stability of the system before proceeding to the next stage. The steps in this stage consist of (1) implementation, namely the system design that has been created is translated into program

ITDM: Information Technology Development And Management
Volume 2, (2) 2026, p. 67-78
E-ISSN: XXXX-XXXX
©2026. The Author(s). This is an open acces article under cc-by-sa

code. Each module is developed and tested individually to ensure that the basic functions can run according to requirements. If during the implementation process deficiencies or inconsistencies with the design or system requirements are found, improvements are made by returning to the previous stage to make adjustments, so that the final results obtained are more optimal. (2) Testing, namely after the implementation stage, it enters the testing phase. Application testing uses the Black Box testing and User Acceptance Testing methods.

D. Transition

This is the final stage, encompassing the system completion process, including documentation and deployment or installation, to ensure the system is ready for use. In this study, the deployment was conducted on a local environment (localhost), not on a public hosting or server. This was done to conduct testing and ensure that all system functionality is running as required. Thus, the transition stage matures the final product, even though it is still on a local trial scale, before being implemented on a live production server.

IV. Result

A. Inception

Business Modeling: Based on observations and interviews, it was discovered that the Finance Department of the Lebak District Ministry of Religious Affairs Office does not yet have an integrated employee database system. All employee information needs still rely on the Human Resources Department. This dependency impacts work efficiency, particularly in financial administration, which requires fast and accurate employee data. Furthermore, the process of printing payslips is still manual. Employees requiring payslips must submit requests directly to the Finance Department. Staff then verify the data and print the payslips individually. This process is time-consuming and dependent on the availability of the relevant staff. Therefore, a proposed system visualized using Business Process Modeling and Notation (BPMN) is needed.

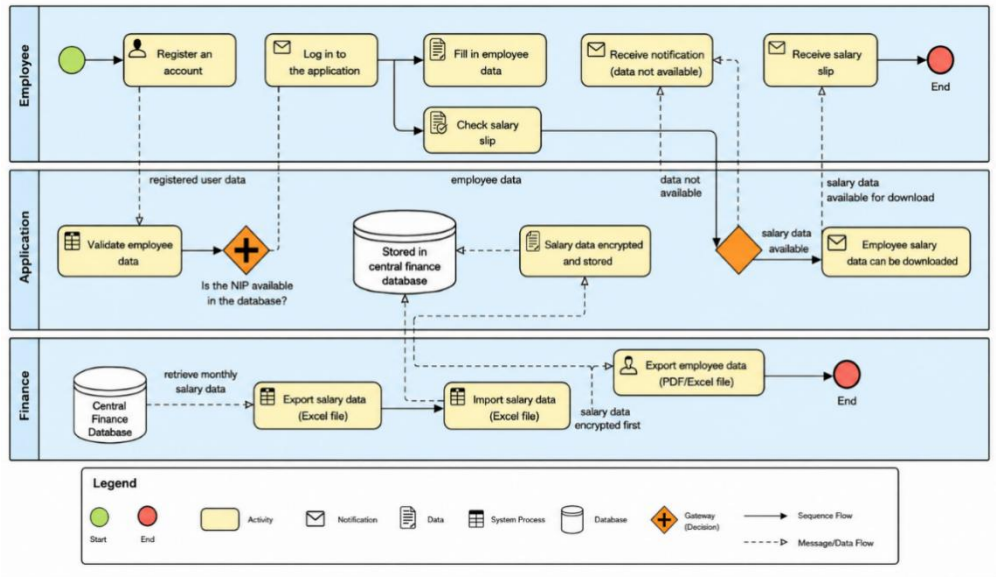


Fig 1. Proposed Business Process Model and Notation (BPMN) System

The proposed system focuses on the Finance Section by providing a special database that does not include other agencies outside the Lebak Ministry of Religious Affairs. Therefore, it is necessary to develop an application that meets the following requirements:

ITDM: Information Technology Development And Management
Volume 2, (2) 2026, p. 67-78
E-ISSN: XXXX-XXXX
©2026. The Author(s). This is an open acces article under cc-by-sa

a. Functional Requirements
- New user account registration
- Forgot password feature to help users who have forgotten their passwords
- Login and logout authentication for administrators and users
- User and administrator profile management
- Family data management (spouse and children)
- Access to salary data and pay slips (download/view).
- Data management by admin (CRUD data for employees, families, salaries, and treasury data).

b. Information Requirements
- Users can update their profiles, family data, and access pay slips.
- Admins can manage employee data, family data, salary data, and update treasurer data

c. Key feature requirements
- General: registration, login, forgot password, profile, logout.
- Admin: Dashboard, user data, family data, pay data (upload from Excel, export reports), settings (change password and treasurer data).
- User: Family data (edit/update), pay data (acces and download slips), settings (change password).

d. Device requirements
- Hardware: Laptop Acer Aspire A314-22, processor AMD 3020e, RAM 4GB, Windows 10.
- Software: Windows 10, Chrome browser, Bootstrap 4 (CSS framework), MySQL (database), and Visual Studio Code (editor).

These specifications were chosen because they are lightweight, easy to implement, and suitable for web-based application development in the environment of the Finance Section of the Ministry of Religious Affairs in Lebak.

B. Elaboration

During the elaboration stage, system analysis and design were carried out using UML (Unified Modeling Language). Several diagram models were used, including Use Case Diagram, Activity Diagram, Sequence Diagram, and Class Diagram.

a. Use Case Diagram

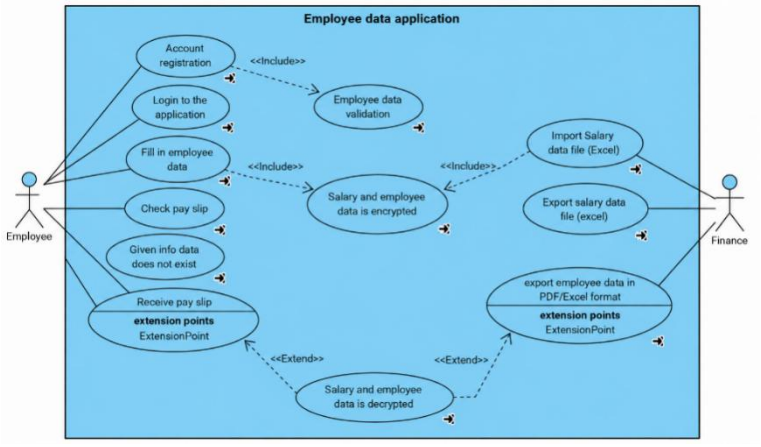


Fig 2. Application Use Case Diagram

ITDM: Information Technology Development And Management
Volume 2, (2) 2026, p. 67-78
E-ISSN: XXXX-XXXX
©2026. The Author(s). This is an open acces article under cc-by-sa

A summary of the use case scenarios is shown in Table

Table 1. Use Case Scenario

No	Use Case	Description	Actor
1.	Account registration	Actor activity to create an account to access the application	Employee
2.	Log in to the application	Actor activity to log in to the application using a username and password	Employee
3.	Fill in employee data	Actions taken by actors to fill in employee data in the application	Employees and admins
4.	Check pay slip	Actions taken by actors to view pay slips	Employees
5.	Receive pay slip	Actions taken by actors to receive pay slips	Employees
6.	Import salary data file	Actions taken by actors to import Excel files containing salary data into the database	Administrator
7.	Export salary data file	Actions performed by actors to export payroll data from the central database of the Ministry of Religion	Administrator
8.	Export employee data file	Actions performed by actors to export employee data files from the application	Administrator
9.	Validate employee data	Actions where the application or system first validates existing data in the database	Employees
10.	Encrypt payroll and employee data	Activity where employee files or data are encrypted before being entered into the database	Administrator
11.	Decrypting salary and employee data	Salary and employee data in the	Administrator

b. Activity Diagram

Activity diagrams are used to illustrate the flow of system processes. These diagrams include the registration process, login, forgotten password, profile management, family data, salary data, and data management by administrators (users, employees, family, salaries, and treasurers).

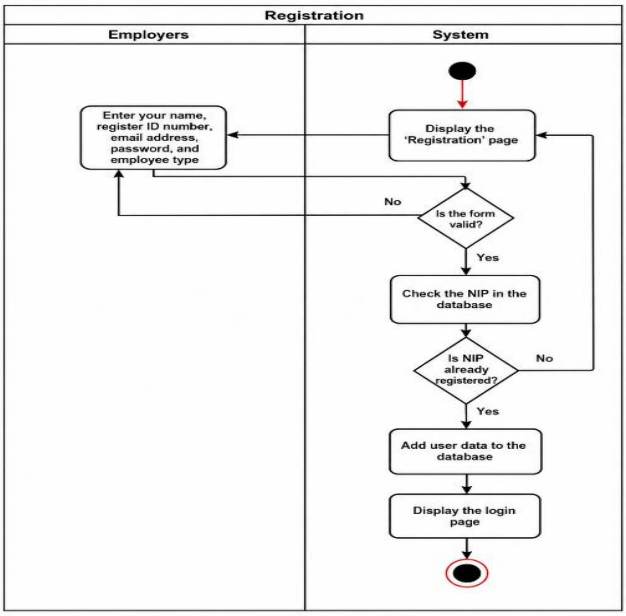


Fig 3. Activity Diagram of Registration

ITDM: Information Technology Development And Management
Volume 2, (2) 2026, p. 67-78
E-ISSN: XXXX-XXXX
©2026. The Author(s). This is an open acces article under cc-by-sa

For example, the Registration Activity Diagram illustrates the process of creating a new account that is verified based on the employee's NIP before the data is stored in the database. The diagram shows that the activity begins when an employee opens the registration page. The employee then fills in personal data such as name, employee ID number, email address, and password. The system will validate the data, for example, checking whether the employee ID number is already registered or whether the email address format is valid. If the data is invalid, the system will display an error message and ask the user to correct the data. If the data is valid, the system will save the information to the database and notify the user that the registration was successful.

c. Sequence Diagram

Sequence diagrams are used to illustrate the interactions between objects in the system during the registration process.

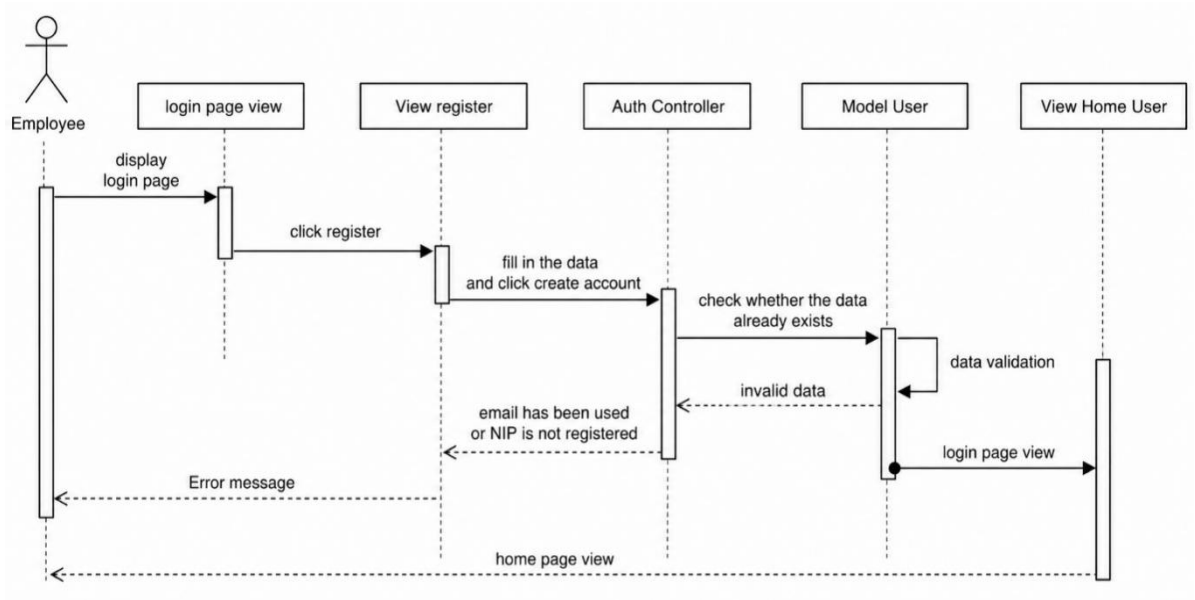


Fig 4. Sequence Diagram of Registration

In this diagram, employees access the registration page and then submit their registration data to the system. The system validates the data. If there are any errors, the system returns an error message to the employee. If all data is correct, the system stores the data in the database and sends a confirmation that the registration was successful.

C. Construction

The application database was built using MySQL DBMS with a total of 7 tables, in accordance with the previous design. These tables include employee data, family data, salary data, user accounts, and other supporting tables. To maintain the security of sensitive data such as NIK, address, telephone number, and other employee data, the system implements encryption using the AES-128 CBC mode algorithm. The employee data encryption and decryption process scheme is shown in Figure 6 in the form of an AES-128 CBC flowchart.

ITDM: Information Technology Development And Management
Volume 2, (2) 2026, p. 67-78
E-ISSN: XXXX-XXXX
©2026. The Author(s). This is an open acces article under cc-by-sa

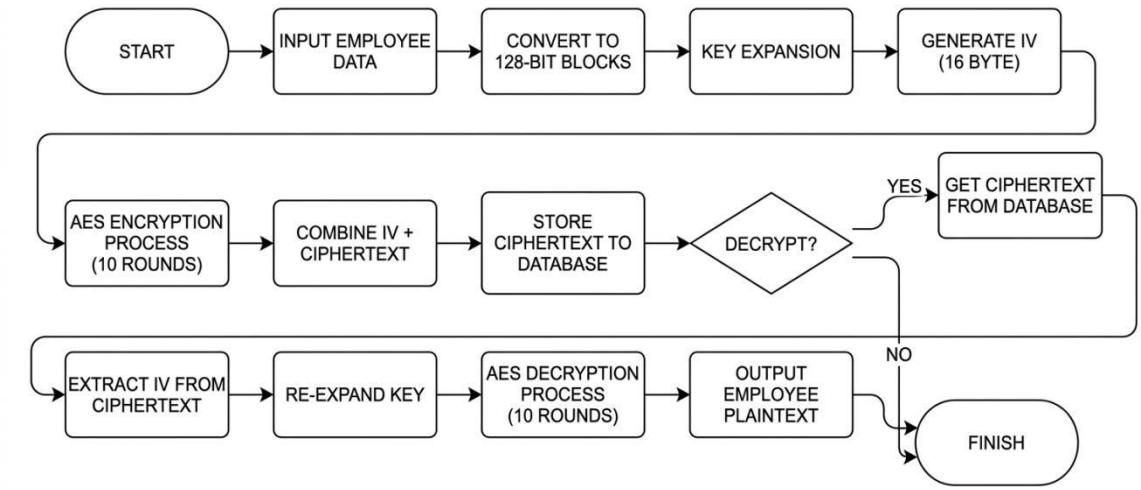


Fig 5. Encryption and Decryption Flow

The employee data management application was successfully built using PHP and MySQL, with integration of the AES-128 CBC algorithm for encrypting sensitive data such as NIK, address, and phone number. The encryption and decryption mechanisms were tested directly through observation of data in the database, where data is stored in ciphertext form and can be correctly converted back to plaintext.

id	taxpayer_id	address	birth_date	gender	phone_number
kiKTjTpH8XSqZEZL88LBIDo3sM3ppy42vljaG4lerm44rwYWGcS...	1234567890123456	nZ3+nzQvMnKx4xSUTNNx3MVw=Oh9g5a5F4TTZWwn4=	2003-03-26	NULL	av57548mhTcBLbLRbmZvLlsg7BKSr
+QVBFgU+mffw7/NgurrELGVBSvwl44+095GGVvWQvTViTmFYC	2345678901234567	G4EXY89qlcMa5go2LEX9WBV8S6uM15mwwWrvBQ=	2003-03-26	female	v7RaZrfaKQAmOD2LYYglQCbBvwaF
ddleSF4a5aXX3P38C3g3WQ2PnDx1yI1yWNG26mdkZgITDDCOk...	3602101407810003	kKSd7YxX4CRWCKXylScfINjJWwkO3KQ4WQ4mFfWWGk=	1981-07-14	male	lakiaYqRqppScAc77Y02v2Yyr9FjNvs
k/1MwxyZkz1+lICyyxpBgTTAWarC44urHacFaceFBeBlrnaBG	1234	cDisEZQqoG6meyQxWQKgzEiXZLJKxoFQv1lyO1G9Jy66=	2003-03-26	female	ayCzS2i778tys3f3ykp3BKaal962mBC
HdfSdJPDOJBDjVfCcDxprfQMkTHP1& afechw9PBvBp1Jcna...	1234567890123456	gm7rtbQcoo4ffC46ZεGpik2PRRbGBeJFHjOnJEN4=	1981-07-14	male	lakiHinpqrlOGQOvVUDnNZEfInexwC

workunit_code	child_code	year
aUoJYkB7PLWzI1PYj/1+Zxt1wHl4Th0CVX+rH6eZEwCv=	aSAh0hEktA0ytxlXEJWDTeKkrKVCiHeFOjyGayIDj6=	lXhzB3IosBA2QQROsFdvRZlmHpFnMTS281HT85FjnEEc=
o8gk9kdJu1CMnR+/EvffEh4kceJ10Qqpk3NV+BqG+FKQ=	akmOSpjgAlxvieHIlV6SHmRBRox4AVFAyRVrsc3H3wo=	RJ5utZemLlKV5giij/VFdDG+pD2ZAZWVHN81E23V/Ag=
UVlMzx8Z9aH0oOwLqII8eCyDduQTil8XAW7aay3R6i8=	Fy3210qySgpc99hhsOg5c5oqy166bltAhQ4kqhygRPg0=	JUWY4yfo5spZUl7etRi68zSx8DQ/Oc0ezW+xngJ6WHM+
RucoAHcXUxLmp6FlvL+4X4uFUf01uGkn8PLTpt4wvO=	jSMBoqtEyQmk5UvVvFHEM+16gM6I4Ua64bu1CBbrilU=	HVDSSksrvsiv6makyutDPkKV9gm2JdX1wr7t70UnNN+M=
PisPZS4QNQXSMyGoVKW4m5PPI1G543/RdUa3WmH3vao=	ZNPe9q7IDwCIFW1abmePer6Ci6wYSSx3lHHxVGIlpU=	jv7jv/mhC6SjopJlwe89QZoKyE3exOuBQW1swwqyhYg=
ijeXIQYPIVXxuOqcTQLVrG5rmsGT8GGTWwj1IlQyQjo=	qzRt+ODcXqeoglq5XZ7gVRXRVms4Nm2H21AaSgb2ym4=	zBzPpSRSRwFb3GZbTirmsprJIlLMBLSLlO3FKTogLKqD0=
shEAIJ7vCp8SROvVlSVCesSx5cRCn4gCJISNMHACtQ5I=	PJ3zcTf557M5JMEA8rhvN6rLlWHTlmCkaVlwmFHXVIY=	r9Kn9ip3bZJgi8HlNF3DjSIFJEm2dH5GuRs1LUpZa7g=
gYdVEBnMvpULgE0ctluvgFvTYLKpShaQlotDNyhMTWc=	vLipLF573UKy4uNkJlOl9Mywhc8EfbW+Map0MSWwegl=	r9CEmuonQUBKebmaJMqSwlQ0xAv2rffS9WGolUl54Sc=
jEmzo0gZXcZPNXLhOPsQirTQqSkNvndLimyOHgt4DKE0=	ElKummiKoDlij7MHuEcbwthhSVrUpyXLxOXV4nXc1lo=	2x9GNTa0ksAE0nU3CwVa6aOPD1HA3YPmTimbSLbck=
mJCBSd+m8Q4EwUprDrj53JI3at4ceWHL1FVhO5MDIPU+	+mGgHfmiq2R3HdviDFSij37krUddrakxMyThlyAdZJYo=	WceZbabgfyF1LDns32QnzpLN12BgROFxDGophyDqcXk=

Fig 6. Employee Data Encryption Results in the Database

UAT testing was conducted on five respondents who used the application. Respondents were asked to answer ten questions using a Likert scale (1–5).

Table 2. Total UAT Test Score

Question No	Total Score (TS)	Maximum Score (SM)	Percentage Score %
1	21	25	84%
2	24	25	96%
3	24	25	96%
4	24	25	96%
5	23	25	92%
6	23	25	92%

ITDM: Information Technology Development And Management
Volume 2, (2) 2026, p. 67-78
E-ISSN: XXXX-XXXX
©2026. The Author(s). This is an open acces article under cc-by-sa

7	24	25	96%
8	23	25	92%
9	24	25	96%
10	23	25	92%
Average Score (%)	93,20%		

The test results show that the application obtained an average score of 93.2%, which falls into the excellent category. This means that the application was very well received by users and is considered to have met the needs of the Finance Section of the Lebak District Ministry of Religious Affairs.

D. Transition

After the development and testing processes were completed, the application was deployed on a local environment (localhost) using the XAMPP web server, which consists of Apache and MySQL. The deployment process included storing the application files in the htdocs directory, importing the database structure via phpMyAdmin, and configuring the .env file to store database connection parameters and AES secret keys. The application can be accessed via a browser at the address http://localhost/nama-folder, and all functionalities, from login, employee data management, payroll slip generation, to data encryption/decryption processes operate as required. To support this explanation, the application documentation is displayed through one example screenshot which serves as a representative illustration that the system can operate according to the organization's needs.

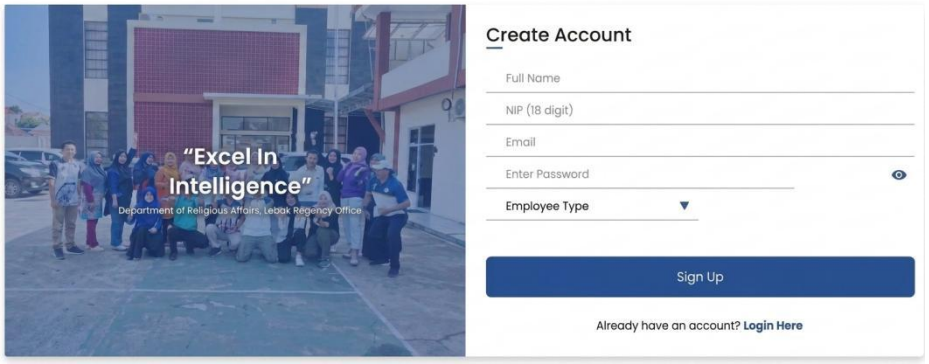


Fig 7. Registration Page

V. Conclusion

An employee data management application has been successfully developed with the aim of supporting personnel administration processes and payroll slip generation in the Finance Section of the Lebak Regency Ministry of Religious Affairs. This application has undergone testing and can run as needed, thereby improving the effectiveness and efficiency of employee data management. Testing results using the User Acceptance Testing (UAT) method showed an average user satisfaction rate of 93.2%, indicating that the majority of users agreed and were satisfied with the performance of the implemented application.

Additionally, to address the need for protecting sensitive data, the application is equipped with security mechanisms such as encryption using the Advanced Encryption Standard (AES) 128-bit algorithm with Cipher Block Chaining (CBC) mode. The implementation of encryption on sensitive data such as NIK, address, and phone number at the database level is expected to minimize the risk of data leakage or loss of employee data.

ITDM: Information Technology Development And Management
Volume 2, (2) 2026, p. 67-78
E-ISSN: XXXX-XXXX
©2026. The Author(s). This is an open acces article under cc-by-sa

Declaration

AI Statement
The authors declare that generative AI tools were used solely to assist with language editing and grammatical improvement. All research ideas, analyses, interpretations, and conclusions are the authors' own. The authors take full responsibility for the content of this manuscript.

Author contribution
Hendra Bayu Suseno: Original Draft, Writing,
Rizqi Laeli and Mohammad Liyananta Septipalan: Editing
Hendra Bayu Suseno: Supervision
Feri Fahrianto, Victor Amrizal and Andrew Fiade: Reviewing

Funding statement
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflict of interest
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Additional information
No additional information is available.

REFERENCES

[1] S. Utama, D. E. Purwoleksono, and T. Rachman, “Data leakage of the Indonesian Elections Commission in legal aspects of personal data protection,” *MI*, vol. 7, no. 3, pp. 479–498, Oct. 2024, doi: https://doi.org/10.20473/mi.v7i3.55931.

[2] A. H. Satria Nusantara, I. Kahirul Umam, and M. Lubis, “Jaminan informasi dan keamanan yang lebih baik: Studi kasus BPJS Kesehatan,” *Nuansa Informatika*, vol. 18, no. 2, pp. 120–127, Jul. 2024, doi: https://doi.org/10.25134/ilkom.v18i2.202.

[3] M. Fathur, “Tanggung jawab Tokopedia terhadap kebocoran data pribadi konsumen,” in *Proc. 2nd Nat. Conf. Law Studies: Legal Development Towards a Digital Society*, vol. 2, 2020.

[4] D. A. Tanjung and M. I. P. Nasution, “Strategi keamanan data dalam database relasional: Tinjauan literatur,” *Jurnal Manajemen Bisnis Era Digital*, vol. 2, no. 2, Art. no. 2, May 2025, doi: https://doi.org/10.61132/jumabedi.v2i2.518.

[5] E. Rustamaji, S. Erbeliza, E. Rahajeng, N. Nuryasin , O. A. Pratama, “Application Security Analysis Mobile Commerce With Mobile Security Framework(MOBSF) and OWASP Mobile Application Security Testing Guide(MASTG)”, Vol. 2, No.1, p. 15-25, April 2026.

[6] Y. H. Syahputra, A. Azlan, and L. A. Girsang, “Pengamanan data penggajian menggunakan Vigenere Cipher pada Mom’s Kitchen Medan,” *J-SISKO TECH (Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD)*, vol. 5, no. 1, pp. 1–6, Jan. 2022, doi: https://doi.org/10.53513/jsk.v5i1.4766.

[7] A. P. Pradhipta and I. G. N. K. Yudiantara, “Analisis regulasi perlindungan data pribadi terhadap kasus kebocoran data di Indonesia,” *Jurnal Media Akademik (JMA)*, vol. 3, no. 7, Jul. 2025, doi: https://doi.org/10.62281/v3i7.2496.

©2026. The Author(s). This is an open acces article under cc-by-sa

[8] A. A. Permana and L. A. Pratiwi, "Implementation of The Advanced Encryption Standard (AES) Algorithm for Digital Image Security", Vol. 15, No. 1, pp. 44-51, 2022. DOI: https://doi.org/10.15408/jti.v15i1.25735

[9] E. E. Awal, E. H. Nurkifli, and T. N. Padilah, "Analisis perbandingan hasil enkripsi dan deskripsi algoritma kriptografi Rijndael dan Twofish untuk penyandian data," *Jurnal Mahasiswa Ilmu Komputer*, vol. 3, no. 1, Mar. 2022.

[10] K. Assa-Agyei and F. Olajide, "A comparative study of Twofish, Blowfish, and Advanced Encryption Standard for secured data transmission," *Int. J. Adv. Comput. Sci. Appl. (IJACSA)*, vol. 14, no. 3, 2023, doi: https://doi.org/10.14569/IJACSA.2023.0140344.

[11] V. P. Brahmaiah, P. V. Jaswantth, D. S. Likhitha, and M. Sudha, "Implementation of AES algorithm," *SciSpace*, accessed Jan. 28, 2025. [Online]. Available: https://typeset.io/papers/implementation-of-aes-algorithm-8fwd5freio

[12] A. Nugrahantoro, A. Fadlil, and I. Riadi, "Optimasi keamanan informasi menggunakan algoritma Advanced Encryption Standard (AES) mode Cipher Block Chaining (CBC)," *FIFO*, vol. 12, no. 1, p. 12, Jul. 2020, doi: https://doi.org/10.22441/fifo.2020.v12i1.002.

[13] Y. I. Chandra, D. R. Irawati, and M. Riastuti, "Penerapan model Rational Unified Process (RUP) dalam membangun aplikasi promosi dan penjualan berbasis web (studi kasus: Toko Mie Ayam 'Neng Kene Kiyeh')," *IKRAITH-Informatika*, vol. 8, no. 3, pp. 107–120, Oct. 2024, doi: https://doi.org/10.37817/ikraith-informatika.v8i3.4369.

[14] N. Nuryasin, P. Y. Presilia, N. M. Maryam, F. Marwahdiyanti, "The Influence of System Security Technology and Data Privacy on User Trust and Satisfaction in Digital Wallet Applications: Systematic Literature Review", Vol. 1, No. 1, p. 42-52, 2025.

[15] M. Prabowo, *Metodologi Pengembangan Sistem Informasi*. Salatiga, Indonesia: Lembaga Penelitian dan Pengabdian kepada Masyarakat (LP2M) IAIN Salatiga, 2020.