Article

File Security Design in Electronic Health Record (EHRs) System with Triple DES Algorithm (3DES) at Jember Family Health Home Clinic

Muhammad Yunus [1], Intan Sulistyaningrum Sakkinah [2], Ulfa Emi Rahmawati [3]*, Atma Deharja [4], Maya Weka Santi [5]

[1] Department of Health, Politeknik Negeri Jember, Jember, 68101, Indonesia; m.yunus@polije.ac.id
[2] Department of Information Technology, Politeknik Negeri Jember, Jember, 68101, Indonesia; intan.sakkinah@polije.ac.id
[3] Department of Information Technology, Politeknik Negeri Jember, Jember, 68101, Indonesia; ulfaemi@polije.ac.id
[4] Department of Health, Politeknik Negeri Jember, Jember, 68101, Indonesia; atma_deharja@polije.ac.id
[5] Department of Health, Politeknik Negeri Jember, Jember, 68101, Indonesia; mayaweka@polije.ac.id
* Correspondence: ulfaemi@polije.ac.id

Citation: M. Yunus, I. S. Sakkinah, U. E. Rahmawati, A. Deharja, and M. W. Santi, "File Security Design in Electronic Health Record (EHRs) System with Triple DES Algorithm (3DES) at Jember Family Health Home Clinic", *IJHIS*, vol. 1, no. 1, pp. 1–8, May 2023.

Received: 10-04-2023
Revised: 10-05-2023
Accepted: 11-05-2023
Published: 12-05-2023

Abstract: Electronic Health Record (EHR) is an electronic version of a patient's medical history maintained by a health care service from time to time. The hacking of medical record data by irresponsible parties is a security threat to the EHR system, including the EHR system belonging to the Jember Family Health Home Clinic which is not equipped with a file security system. This research was conducted by designing file security on the EHR system with the Triple DES (3DES) algorithm using UML (Unified Modeling Language) diagrams. The Triple DES (3DES) algorithm was chosen because it is considered secure in securing files. The results of this study are the design of adding file security with 3DES to the EHR system to help maintain the confidentiality of vital medical record data. Further research can be done by building a file security system using 3DES according to the design that has been made.

Keywords: Decryption, Electronic Health Record, Encryption, Medical Record, Triple DES

1. Introduction

The health sector in Indonesia has shown very significant growth in the use of information technology in health services. This can be seen in the development of electronic medical records (EHR) as a form of use of information technology in healthcare [1]. Implementing an EHR can improve healthcare delivery and positively impact patient care and treatment [2]. An electronic medical record (EHR) is an electronic version of a patient's medical history maintained by a healthcare provider from time to time and may contain all important administrative clinical data including demographics, progress records, questions, medications, vital signs and medical history, past health, immunizations, laboratory and radiological data [3].

Cyber-security methodologies related to the implementation of Electronic Health Records (EHR) must also be applied because as many as 70% of people are worried that their health information will be leaked. This is evidenced by the sale of patient data at the University of Chicago Hospital and Wilcox Memorial Hospital, Kauai, Hawaii (130,000 patient data) [1]. In Indonesia, there are still some health data leaks. Millions of patient data from sharing hospitals on the server of the Ministry of Health allegedly leaked and sold on the dark site RaidForums on January 6, 2022. In addition, as many as 279 million participant data of the Social Security Administering Body or BPJS Kesehatan allegedly leaked in 2021. Report Indonesia Cyber The Security Independent Resilience Team (CISRT) stated that material losses from the leak of 279 million BPJS Health participant data reached Rp 600 trillion.

Hacking of Electronic Health Records (EHR) data by irresponsible parties is a security threat to the Electronic Health Records (EHR) system [4]. Leaked patient data has the potential to encourage fraud with phishing methods against data owners. Perpetrators can reveal the disease of patients who have leaked data or certain medical conditions that are confidential [5]. In Indonesia, some laws regulate privacy security, namely the Information and Electronic Transactions Law (ITE) in articles 5 and 6 [6], as well as the Minister of Health Regulation Number 269 of 2008 concerning Medical Records article 2 [7].

Family Health Home (RSK) is one of the Health Clinics in Jember Regency which is managed by a social foundation. Previous research conducted by Muhammad Yunus, Atma Deharja, and Maya Weka Santi (2021) under the title "Designing Electronic Health Records (EHRs) in a Jember Family Healthy Home Clinic" resulted in an EHR system, but currently, the EHR is not equipped with a security system. medical record data [8]. So, it is very possible for the theft of data or patient medical information in the system database.

Another study conducted by Bagas Putra Pratama & Wasis Haryono (2020) under the title "Designing Cryptographic Applications on Archiving Documents Using the WEB-Based Triple DES Algorithm" discusses the security of document archiving using the Web-based Triple DES algorithm. This is because there are still many irresponsible parties who can access files freely. So that a web-based application is built that can provide file security using the Triple DES algorithm [9].

So, from the description and previous research, research related to the design of file security in the Electronic Health Records (EHR) system with the Triple DES (3DES) algorithm was carried out at the Jember Family Health Home Clinic. The results obtained from this study are the design of adding file security with the Triple DES (3DES) algorithm on the Electronic Health Records (EHR) system to be able to help maintain the confidentiality of medical record data at the Jember Family Health Home Clinic. The Triple DES algorithm is a strong encryption system in terms of data security, access control systems, and passwords. So that no party is harmed because medical record data is safer. This research is structured as follows: Part 1 contains an introduction. Section 2 contains materials and methods. Section 3 contains the results and discussion. Finally, Section 4 describes the conclusions and further research.

2. Materials and Methods

The research method used is the descriptive research method or also called the analytical research method. In this descriptive research method, literature studies and observations are carried out on problems related to research.

2.1. Medical Record Data

A medical record is a record file containing patient identity documents, examination results, treatment given, as well as other actions and services to patients [7]. Along with the development of information technology, Electronic Health Records (EHR) began to be developed to store data and information on patient care. and bridge the sharing of information between doctors, patients, and hospitals. With electronic medical records, data is easier to store and can be used to make clinical decisions [10]. Electronic Health Records (EHRs) help improve the quality of health information, especially in the recording, retrieval, and use of health data. Patients can directly benefit from secure and accessible electronic clinical information to make better decisions [11].

Some of the benefits of implementing Electronic Health Records (EHR) are cost savings [12, 13], cost efficiency, and cost-effectiveness [14]. EHR also provides benefits to management, namely facilitating monitoring and evaluation activities. Information obtained from electronic medical records can improve supervision by management on the productivity of medical personnel [15]. The use of electronic medical records aims to reduce medical errors and improve patient safety [16]. Electronic Health Records (EHR) can improve the readability of data because the documentation is done computerized to minimize reading errors and data loss. This of course can improve continuity of care and reporting, accuracy, patient evaluation process, medical research, and policy analysis including the clinical decision-making process [15].

2.2. Triple DES Algorithm (3DES)

Cryptography means data security, helps ensure data privacy, maintains data integrity, authenticates communicating parties, and prevents rejection [17] with a working pattern as shown in Figure 1.

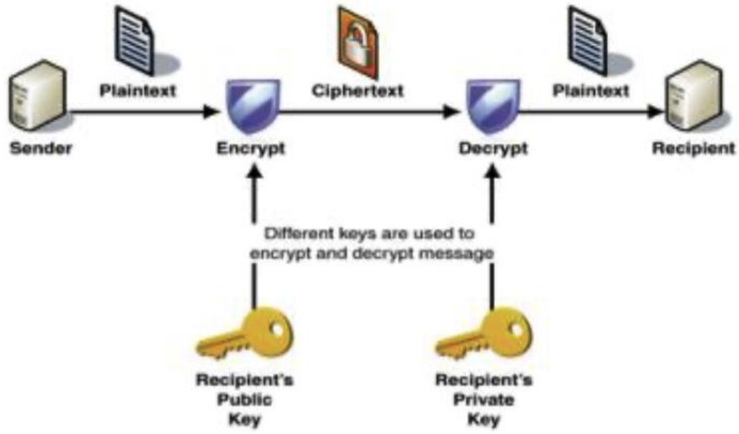

Figure 1. Cryptographic Encryption and Decryption Process [17]

Triple DES is an algorithm in cryptography that uses three iterations of the DES cipher with a 168-bit secret key. Where the secret key is divided into three 56-bit keys [17], as shown in the block diagram in Figure 2.

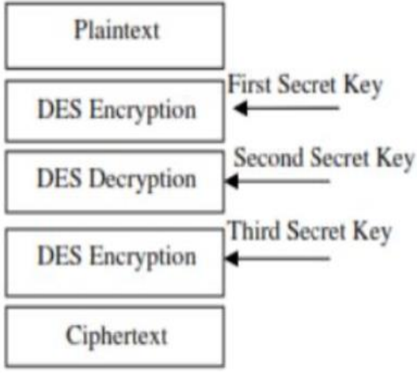

Figure 2. Block Diagram of the 3DES Algorithm [17]

2.3. Unified Modeling Language (UML)

Unified Modeling Language (UML) is a visual modeling method for object-oriented system design tools and UML is also a language that has become a standard in visualization, design, and system documentation [18]. The UML (Unified Modeling Language) diagram used in this study consists of a Use Case Diagram and an Activity Diagram. A use case diagram is a diagram that describes the interaction between one or more actors and the application to be made [19]. Activity diagrams describe a series of the flow of activities, used to describe activities that are formed in one operation so that they can also be used for other activities [20].

3. Results and Discussion

Computer security issues are one of the important aspects of a system. However, this security issue has received less attention from the owners and managers of information systems. One of them is medical record data on the Electronic Health Records (EHR) system at the Jember Family Health Home Clinic. The very importance of the value of medical record data causes many other parties to want to steal the information. If the information falls to another party, it can cause harm to the owner of the information.

Data file encryption problems usually arise when several employees ask the officer (administrator) to keep data about themselves confidential from other parties. Therefore, after the administrator logs in, encryption is used to secure the data in the form of files that you want to keep secret. The encryption itself is the process of scattering the original data into another form that is not easy to guess but can be returned to its original form if needed.

There are so many encryption technologies, one method that is considered strong in doing this security is the Triple DES algorithm method which is encoding by changing the location of the letters in the message to be encoded. And to read the original message again is enough to return the location of the letters in the message based on the key and letter shift algorithm that has been agreed upon by the sender and recipient. Triple DES is basic security published since January 15, 1977, and is often used everywhere, therefore Triple DES becomes a strong encryption system in terms of data security, access control systems, and passwords. Data is encrypted in 64-bit blocks using a 56-bit key. Data is encrypted into 64-bit blocks using a 56-bit key. Triple DES uses multiple levels of encryption to convert 64-bit input to 64-bit output. Using the same steps and keys, Triple DES is used to undo encryption (commonly referred to as the decryption process).

The way Triple DES works on the Electronic Health Records (EHR) system is to perform the encryption process on the admin side and decrypt from the partner side as a third party, more details can be seen in Figure 3. In this study, the function and purpose of adding cryptography to the algorithm Triple DES are to strengthen the security of medical record data on the Electronic Health Records (EHR) Jember Family Health Home Clinic.

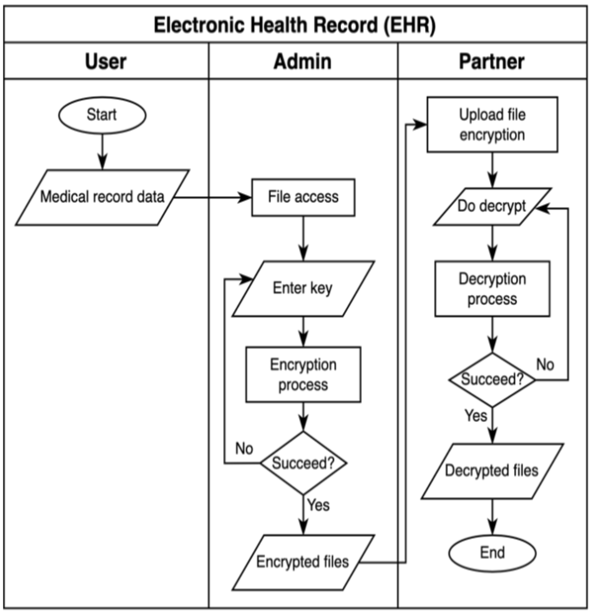

Figure 3. Flowchart of adding cryptography with the Triple DES algorithm

The tools used in designing additional file security with the Triple DES (3DES) algorithm on the Electronic Health Records (EHR) system are UML (Unified Modeling Language) Diagrams. UML, the full name of Unified Modeling Language, is a visual modeling method for object-oriented system design tools. UML is also a language that has become a standard for visualization, design, and system documentation [18]. The UML (Unified Modeling Language) diagram used in this study consists of a Use Case Diagram and an Activity Diagram.

A use case diagram is a diagram that describes the interaction between one or more actors and the application to be made [19]. The use case diagram in the design of additional file security with the Triple DES (3DES) algorithm on the Electronic Health Records (EHR) system is as follows.

3.1. Use Case Diagram of the User

The Electronic Health Records (EHR) system, begins with the user/patient registering an account to be able to register for several services such as clinical examinations and doctors and drug prescription services, for more details, see Figure 4.

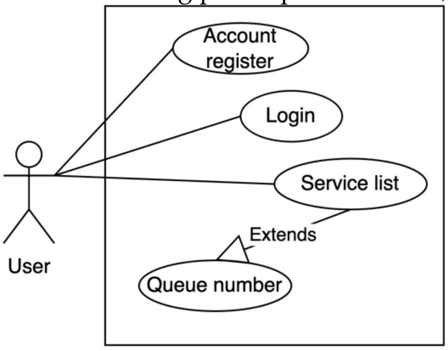

Figure 4. Use case diagram of the user

3.2. Use Case Diagram of Admin

In the EHR application, the admin can encrypt the user/patient medical record data in the Electronic Health Records (EHR) system. The admin first logs in and then encrypt the medical record data before the data is stored as shown in Figure 5.

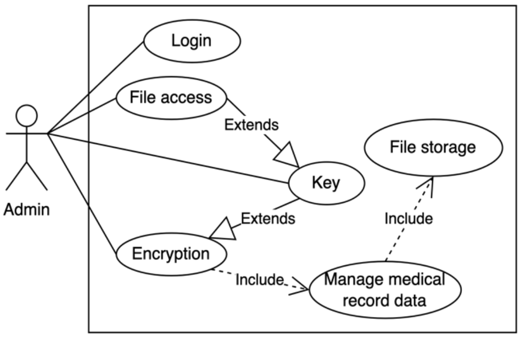

Figure 5. Use case diagram of admin

3.3. Use Case Diagram of Partner

When there is a medical action that cannot be handled by the Jember Family Health Home Clinic, the patient's medical record data is sent by the admin to the referral partner, of course, the admin sends the encrypted medical record data. Partners need to log in to the Electronic Health Records (EHR) system and carry out the process of decrypting the user/patient medical record data before use, for more details, see Figure 6.

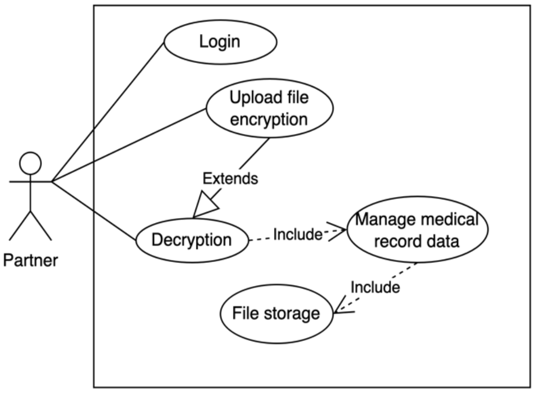

Figure 6. Use case diagram of partner

An activity diagram describes a set of activities that describe the activities formed in an operation so that they can also be used for other activities [20]. This diagram illustrates the activities carried out by the system in carrying out the functions selected by the user.

3.4. Activity Diagram of Login

The login activity diagram is shown in Figure 7. This login is carried out by the user, admin, and partners.

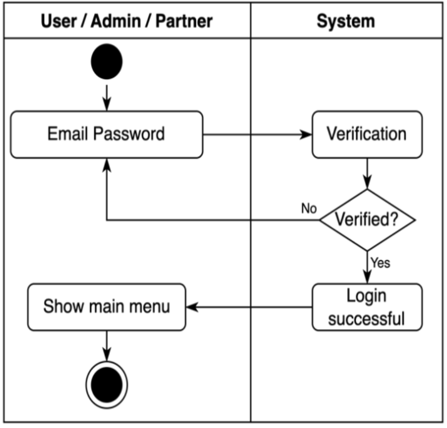

Figure 7. Activity diagram of login

3.5. Activity Diagram of the Encryption

The encryption activity diagram that can only be done by the admin can be seen in Figure 8.

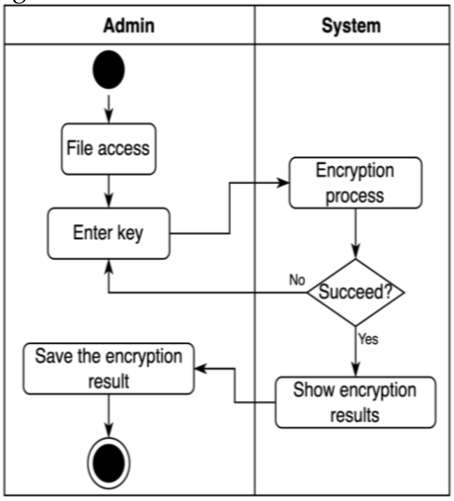

Figure 8. Activity diagram of the encryption

3.6. Activity Diagram of the Decryption

The activity diagram decryption that can only be done by partners can be seen in Figure 9.

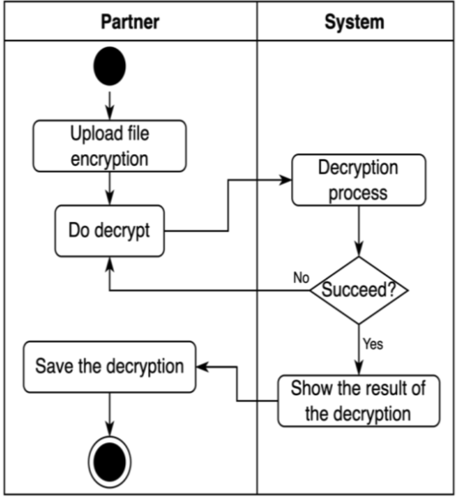

Figure 9. Activity diagram of the decryption

4. Conclusions

An electronic medical record (EHR) is an electronic version of a patient's medical history maintained by a healthcare provider from time to time and may contain all important administrative clinical data including demographics, progress records, questions, medications, vital signs and medical history, past health, immunizations, laboratory and radiological data. These data are very vital and require data security from theft and misuse by irresponsible parties. The method that is considered strong in securing data is the Triple DES algorithm method which is encoding by changing the location of the letters in the message to be encoded. Triple DES is a strong encryption system in terms of data security, access control systems, and passwords. By using cryptographic security on the system, it will prevent data theft from irresponsible people, applying the Triple Des algorithm can also guarantee data security very accurately.

From this research, a design for the application of the Triple DES cryptographic algorithm was made for the security of medical record data on the Electronic Health Records (EHR) system that has been created and used by the Jember Family Health Home Clinic since 2021 from the results of previous research. The way Triple DES works on the Electronic Health Records (EHR) system is to perform the encryption process on the admin side and decrypt from the partner side as a third party.

This research is limited to system design before its implementation. UML (Unified Modeling Language) Diagrams are used to design additional file security with the Triple DES (3DES) algorithm on the Electronic Health Records (EHR) system. The design of adding file security with the Triple DES (3DES) algorithm on the Electronic Health Records (EHR) system is expected to help maintain the confidentiality of medical record data at the Jember Family Health Home Clinic. That way, no party will be harmed because medical record data is safer. Further research can be done by building an encryption system using the Triple DES algorithm according to the design that has been made.

References

1. A. M. Ningtyas and I. K. Lubis, "LITERATUR REVIEW PERMASALAHAN PRIVASI PADA REKAM MEDIS ELEKTRONIK," 2018. [Online]. Available: www.ejournal.unib.ac.id/index.php/pseudocode
2. D. F. Sittig, D. Gonzalez, and H. Singh, "Contingency planning for electronic health record-based care continuity: A survey of recommended practices," *Int J Med Inform*, vol. 83, no. 11, pp. 797–804, Nov. 2014, doi: 10.1016/j.ijmedinf.2014.07.007.

3. C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, "Security Techniques for the Electronic Health Records," *J Med Syst*, vol. 41, no. 8, Aug. 2017, doi: 10.1007/s10916-017-0778-4.
4. Y. R. Priyatna, A. Kusyanti, and M. Data, "Implementasi Algoritme Grain Untuk Pengamanan Data Rekam Medis," 2019. [Online]. Available: http://j-ptiik.ub.ac.id
5. M. H. Wibowo and N. Fatimah, "ANCAMAN PHISHING TERHADAP PENGGUNA SOSIAL MEDIA DALAM DUNIA CYBER CRIME," 2017.
6. Ministry of Communication and Informatics, "Undang-Undang Republik Indonesia nomor 19 tahun 2016 tentang informasi dan transaksi elektronik," in *UU No. 19 tahun 2016*, 2016, pp. 1–31.
7. Ministry of Health Republic of Indonesia, *Peraturan Menteri Kesehatan Republik Indonesia nomor 269/MENKES/PER/III/2008*. 2008.
8. M. Yunus, A. Deharja, and M. W. Santi, "Designing Electronic Health Record (EHRs) in a Jember Family Healthy Home Clinic," 2021.
9. B. Putra Pratama and W. Haryono, "PERANCANGAN APLIKASI KRIPTOGRAFI PADA DOKUMEN PENGARSIPAN DENGAN MENGGUNAKAN ALGORITMA TRIPLE DES BERBASIS WEB," vol. 1, no. 4, 2020, [Online]. Available: http://openjournal.unpam.ac.id/index.php/JOAIIA/index204
10. R. T. Budiyanti, P. M. Herlambang, and N. Nandini, "Tantangan Etika dan Hukum Penggunaan Rekam Medis Elektronik dalam Era Personalized Medicine," *Jurnal Kesehatan Vokasional*, vol. 4, no. 1, p. 49, Feb. 2019, doi: 10.22146/jkesvo.41994.
11. Z. S. N. Reis, T. A. Maia, M. S. Marcolino, F. Becerra-Posada, D. Novillo-Ortiz, and A. L. P. Ribeiro, "Is there evidence of cost benefits of electronic medical records, standards, or interoperability in hospital information systems? overview of systematic reviews," *JMIR Medical Informatics*, vol. 5, no. 3. JMIR Publications Inc., Jul. 01, 2017. doi: 10.2196/medinform.7400.
12. B. Tilahun and F. Fritz, "Modeling antecedents of electronic medical record system implementation success in low-resource setting hospitals Healthcare Information Systems," *BMC Med Inform Decis Mak*, vol. 15, no. 1, Aug. 2015, doi: 10.1186/s12911-015-0192-0.
13. N. A. Mohd Nor *et al.*, "Development of electronic medical records for clinical and research purposes: The breast cancer module using an implementation framework in a middle income country- Malaysia," *BMC Bioinformatics*, vol. 19, Feb. 2019, doi: 10.1186/s12859-018-2406-9.
14. J. E. Hernández-Ávila *et al.*, "Assessing the process of designing and implementing electronic health records in a statewide public health system: The case of Colima, Mexico," *Journal of the American Medical Informatics Association*, vol. 20, no. 2, pp. 238–244, 2013, doi: 10.1136/amiajnl-2012-000907.
15. D. Rizky and A. Tiorentap, "Manfaat Penerapan Rekam Medis Elektronik Di Negara Berkembang: Systematic Literature Review," 2020.
16. G. Deimazar, M. Kahouei, A. Zamani, and Z. Ganji, "Health information technology in ambulatory care in a developing country," *Electron Physician*, vol. 10, no. 2, pp. 6319–6326, Feb. 2018, doi: 10.19082/6319.
17. Karthik S and Muruganandam A, "Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System." [Online]. Available: www.ijser.in
18. A. Yunus and A. Cholirul Rohman, "Sistem pendukung keputusan penentuan lahan pertanian, pertambangan, dan perindustrian (SOFTPLET) dengan menggunakan metode SMARTER," *SMARTICS Journal*, vol. 4, no. 1, pp. 5-10, 2018, doi: 10.21067/smartics.v4i1.2693.
19. T. Bayu Kurniawan and Syarifuddin, " PERANCANGAN SISTEM APLIKASI PEMESANAN MAKANAN DAN MINUMAN PADA CAFETARIA NO CAFFE DI TANJUNG BALAI KARIMUN MENGGUNAKAN BAHASA PEMOGRAMAN," *Jurnal TIKAR*, vol. 1, no. 2, pp. 192-206, 2020, doi: 10.1234/teknik_informatika.v1i2.153.
20. R. Septian Anwar and T. Dwi Cahyono, "Science and Technology PERANCANGAN APLIKASI BERBASIS ANDROID DENGAN METODE ECONOMIC ORDER QUANTITY DI PT. SAMAWA TIRTA ALAM SUMBAWA," 2019. [Online]. Available: http://jurnal.uts.ac.id