Internet Cafe Billing System Data Security Using RC4 Stream Cipher

Bobi Akbar

STMIK Budidarma, Indonesia
Email: kikisaputra@gmail.com

Received: 14 October 2020
Revised: 26 November 2020
Accepted: 27 November 2020

© 2020 The Author: Published by Cattleya Darmaya Fortuna

Abstract
In data communication, against a data security method known as cryptography (Cryptography). Cryptography is a data security method that can be used to maintain data confidentiality, data authenticity or integrity, and the authenticity of the sender. This method is intended so that important information of a limited or confidential nature sent through public telecommunications facilities cannot be known or utilized by unauthorized parties. In this case, data security is also needed at the internet cafe (internet cafe). Warnet which is a place that provides Interconnection Networking that connects computers to form a network system that covers the whole world (global). Each cafe requires a billing system that is used to determine the state of the user in using the facilities at the cafe, starting from how long it takes to use and how much it costs each user. For this reason, so that the data on the billing system cannot be manipulated or modified by unauthorized persons, it is necessary to secure data. The data security method that will be used is cryptography, especially by using the RC4 stream cipher.

Keywords: Data Security, Warnet Billing System, RC4 Stream Cipher

INTRODUCTION

Technological developments, especially in data security systems in maintaining information data security, have grown rapidly[1]. Security issues that are of great concern today, namely the means of data protection, network security, virtualization security, application integrity, and identity management used by services[2]. The data security process is expected to prevent data theft or eavesdropping by hackers, crackers, carders, phreakers, and so on[3]. Data security on computers can provide protection to our data[4] from tapping data[5]. Sending data or information without security will be at risk of eavesdropping[6]. So that the data is safe from unauthorized parties, a Data Security Application is made using cryptographic techniques[7]. The Internet of Things (IoT) is a commercial revolution, and the adoption of IoT devices in enterprises leads to data management success, as well as the organization's success. The use of a business intelligence system is both a technological and a social solution for improving communication and providing quick access to information. Business information security improvements, on the other hand, result in technological and non-technical damages, threats, and activities that are in violation of business information security principles. The primary goal of this research is to investigate the impact of data security on the deployment of business intelligence systems. The RC4 Stream Cipher technique is extensively used because it is simple to implement in a variety of applications and has been confirmed safe.
to use. Encryption using the Rivest Code 4 (RC4) technique is one of the various models and approaches available. The outcome of this study is the use of the RC4 Stream Cipher Encryption program, with the number of original characters (plaintext) successfully encrypted equal to the number of encrypted characters (ciphertext), so that the input data is stored in an encrypted state in the database, ensuring the data's security and confidentiality. The most extensively used stream cipher software is RC4, also known as ARCFour (Alleged RC4). RC4 is also used in well-known protocols as SSL (Secure Sockets Layer), which protects internet traffic, and WEP, which secures wireless networks. Say. The security of messages, data, or information in the process of delivering or storing data is one of the most significant aspects of computer and computer network communication, and it has become one of the driving forces behind the development of cryptographic technology. Cryptography is a data coding technique that supports two elements of information security, namely secrecy and confidentiality. The RC4 Stream Cipher technique is extensively used because it is simple to implement in a variety of applications and has been confirmed safe to use.

METHODS

Data Security
Data is a file that can be confidential so it requires a data security process to maintain its confidentiality. Cryptography is the process of securing data that can be used based on the use of algorithms, one of which is[8]RC4 Stream Cipher. Cryptography is one of the appropriate data security solutions or methods to maintain the confidentiality and authenticity of data, and can improve the security aspects of data or information. Cryptography is a field of science that studies data encoding techniques[9]. Text data is data that has characteristics such as letters, numbers, symbols contained in a document or is a form that does not have objects such as images. Securing text data in the form of ciphertext and the resulting ciphertext results do not increase the capacity of the original data to be one of the commonly known problems that the dominant ciphertext results increase capacity, for that the author tries to secure it with Block Cipher and Stream Cipher[10]. Data security can be done in two ways. The first way is setting the permissions of each user by the database administrator. The second way is data security in terms of data content stored in the database[11].

Internet Cafe Billing System
In this billing, all data is stored in a mysql database, so it can be easier for the owner to see the number of consumers and the length of time consumers make rentals[12]. Billing Hotspot is an application used for managing internet access users, such as recording transactions and monitoring users[13]. The input of this research is data that is sent in real time from the billing machine, from a series of trials that have been carried out it can run smoothly, which is evidenced by measuring data transmission with speed in accessing article data an average of 0.7833 seconds / transaction data manually[14].

RC4 Stream Cipher
The RC4 algorithm (Ron's Code/Rivest's Cipher) is an algorithm that can be used to encrypt data so that the original data can only be read by someone who has the encryption key.[4]. The RC4 stream cipher algorithm is used to convert the actual data into certain symbols, so that the data will not be understood by parties who do not have access rights.[15]. The hardware specifications used for the implementation of making and running the program so that it runs properly are as follows:
1. Processor : Minimum Pentium III-800 Mhz
2. Memory : Minimum 64 MB
3. Hard disk : Minimum 5 GB
4. Graphics Card : VGA 8 MB with SVGA monitor
5. Monitor : SVGA 1924x78 pixels into 16 Bit color.

In making this program required some software, namely:
1. Operating system : Windows 98 SE, Windows ME, or Windows XP
2. Application : Visual Basic 6.0

RESULTS And DISCUSSION

Training Data With VB 6.0
RC4 has an S-Box, S0, S1, ……, S255, which contains permutations from 0 to 255. It uses two indexes, namely i and j in its algorithm. Index I is used to ensure that an element changes, while index j will ensure that an element changes randomly. In essence, in the encryption algorithm this method will generate pseudorandom bytes from the key which will be subjected to XOR operations on the plaintext to produce ciphertext. And to produce the original plaintext, the ciphertext will be subjected to an XOR operation against the pseudorandom bytes. In the following, a chart will be provided illustrating the series of processes that are executed to encrypt or decrypt data.

![Figure 1: RC4 Stream Cipher Process Circuit](image)

The following will explain the parts of the RC4 Stream Cipher algorithm along with its implementation as follows:

- **plaintext** : encryption
- Ascii plaintext : 101 110 107 114 105 112 115 105
- **Key** : computer
- Ascii key : 107 111 109 112 117 116 101 114

Implementation
To run this image processing software, it is enough to run the Billing.exe file, after running it will display a flash display as follows:

![Flash Display](image)

**Figure 2**: Flash Display

This form is used as the main menu of the system, as shown in the image below:

![Main Menu Form](image)

**Figure 3**: Main Menu Form

This menu is a sub menu of the file menu, as shown in the image below:
This menu is a sub menu of the view menu, as shown in the image below:

Figure 4: File Menu

This form is used to perform the process of switching usage between computers, as shown in the image below:

Figure 5: View Menu

This form is used to view encrypted information, as shown in the image below:

Figure 6: Transfer Account Form
Figure 7: Encryption Results

This form is used to view decrypted information, as shown in the image below:

![Encryption Result](image)

Figure 8: Decryption Results

This form is used to view connected client information, as shown in the image below:

![Decryption Result](image)
CONCLUSION

Based on the results of the discussion and program tests, conclusions can be drawn, including:

1. The RC4 algorithm can be used as a data security technique against attacks from unauthorized parties. The use of a long key will be better to create more secure security. In this Billing security, what can be secured is only data on internet usage by the user (user).
2. Microsoft Visual Basic 6.0 programming language can be used as a security program for internet billing data using RC4 Stream Ciper.

REFERENCES

[1] FN Pabokory, IF Astuti, and AH Kridalaksana, "Implementation of Cryptographic Data Security in Text Messages, Document File Contents, and Document Files Using the Advanced Encryption Standard Algorithm," Information. Mulawarman J. Ilm. Computer Science., vol. 10, no. 1, 2016.
[2] M. Ula, "ANALYSIS OF DATA SECURITY METHODS IN CLOUD COMPUTING SERVICES," TECHSI - J. Tek. information., vol. 11, no. 1, 2019.
[3] MI Ukkas, R. Andrea, and ABP Anggen, "DATA SECURITY TECHNIQUES WITH END OF FILE STEGANOGRAPHY (EOF) AND VERNAM CIPHER CRYPTOGRAPHY," Sebatik, vol. 17, no. 1, 2017.
[4] DR Saragi, JM Gultom, JA Tampubolon, and I. Gunawan, "Securing Text File Data (Word) Using the RC4 Algorithm," J. Sis. computer. and Information., vol. 1, no. 2, 2020.
[5] M. Syahril and H. Jaya, "Application of Steganography for Customer Data Security at Standard Chartered Bank Using Least Significant Bit and RC4 Methods," Semin. Nas. Technol Science. inf., 2019.
[6] R. Toyib and Y. Darnita, “Securing Text Data Using Zero-Knowledge Proof Algorithm,” J. MEDIA INFOTAMA, vol. 16, no. 1, 2020.
[7] R. Prasetyo and A. Suryana, "Data Security Application with AES Cryptographic Algorithm Technique and Desktop-Based SHA-1 Hash Function," J. Sisfokom (Inf.
[8] S. Permatasari, A. Aminudin, and S. Arifianto, "Modification of AES Encryption and Decryption with Polybius Cipher in Data Security," *JRST (Journal of Ris. Science and Technology)*, vol. 4, no. 1, 2020.

[9] S. Widyastuti, W. Ariandi, and V. Sulistiono, “Implementation of AES Cryptography in Security of JAMKESMAS Participant Selection Data,” *J. Ilm. Intech Inf. Technol. J. UMUS*, vol. 1, no. 02, 2019.

[10] D. Kurniawan, "PLANNING OF TEXT DATA SECURITY APPLICATIONS USING BLOWFISH AND RC6," *J. Pelita Inform. ISSN 2301-9425 (Print Media)*, vol. 17, no. 3, 2018.

[11] D. Ekklesia, "Study and Implementation of Database Security with Stream Cipher Cryptography Techniques," *SAINTEKBU*, vol. 3, no. 1, 2016.

[12] Z. Reno Saputra, T. Ismail, HM M, and HP M, “DESIGN OF BILLING PLAYSTATION SYSTEMS BASED ON ARDUINO-BASED PLAYSTATION BILLING SYSTEM DESIGN,” *Jusikom J. Sist. computer. Musirawas*, vol. 4, no. 02, 2019.

[13] MY Setiawan, "Design and Implementation of Hotspot Billing Using PHP and Api on Mikrotik at Cybercity Networks," *library. UNIKOM*, no. 2014, 2016.

[14] R. Dimas Adityo and H. Miawarni, "Application of Cloud Computing Based POS (Point Of Sales) Billing Applications for Restaurant / Restaurant Managers By Utilizing IoT (Internet Of Thing) Devices in Probolinggo Regency, East Java," *Sentia 2018*, vol. 10, no. 1, 2018.

[15] SA Agusta and TA Fitri A, "Implementation of the RC4 Stream Cipher Algorithm in the Application for Data Collection for Alumni STMIK Amik Riau," *INOVTEK Polbeng - Inform Series.*, vol. 1, no. 1, 2016.