Login Security Using One Time Password (OTP) Application with Encryption Algorithm Performance

Dwi Ely Kurniawan1*, Mohd Iqbal2, John Friadi3, Fendi Hidayat3, Ririt Dwiputri Permatasari4

1Department of Informatics Engineering, Politeknik Negeri Batam, Indonesia
2Department of Informatics Engineering, STIKOM Muhammadiyah Batam, Indonesia
3Department of Information System, Universitas Batam, Indonesia
4Faculty of Engineering, Universitas Ibnu Sina, Indonesia

*dwialikhs@polibatam.ac.id

Abstract. During the Covid-19 pandemic, almost all jobs and activities to be limited, relying on the internet network. Data security in an internet network is most important and needs to be a concern for internet users. The internet network is a public network, which is vulnerable to security attacks. Attacks may occur to retrieve user data in the form of a username and password. This study conducts system design to improve the security of the username and password data when logging into web applications. Login using One-Time Password (OTP) verification by implementing the AES algorithm and Blowfish to encrypt the verification code. The verification code uses an SMS gateway. Testing is done by looking at security performances and comparing the performance of the Blowfish and AES algorithm. The results of the design research show that OTP is running well where the AES algorithm performance has advantages in terms of encryption and decryption speed compared to the Blowfish algorithm with a difference of ± 0.015 milliseconds for encryption and ± 0.04 milliseconds for decryption.

1. Introduction

The development of communication devices makes it easier for a person to communicate over long distances by sending text, voice, image, and video information over the internet network [1]. Especially during the Covid-19 pandemic, almost all jobs and activities to be limited to using the internet [2]. Without having to go out of the house. The internet is a network of computers that are connected. Communication across public networks such as the internet has the potential for data theft or alteration by unauthorized parties [3]. Therefore, tools for the login security of data must be available. Confidentiality of information data sent or received is the most important thing so that only certain people can access that information data. One of the problems in information data security [4] is that when a user identifies himself in a web application [5], the web application needs to verify the user's identity. The way to authenticate users on the web application is by using a password [6]. Static passwords are codes that frequently use multiple times to log into web applications, leaving them vulnerable to account security.

Based on the results of sharing vision research to 151 social media [7] respondents, it shows that 13.6% of the passwords are known to others, and 9.9% of account theft. The 2017 Data Breach
Investigation Report (DBIR) contained 81% of hacks using passwords [8]. Some of the criminal techniques used to get passwords are sniffing [9], which is a wiretapping activity carried out on the network, so that to maintain the confidentiality of information data, data security is required. Data security guarantees the login security of applications in the internet network. The application of login security can provide through login verification. This verification means providing a code via another device such as an SMS, token [10], or something else [11].

This study aims to design a login security application using One Time Password (OTP). OTP is a login verification code that is only used for one login. The OTP verification code is sending through a gateway server equipped with an encryption algorithm. Previous research about One Time Password (OTP) are studies modified 256 bit AES algorithm to activate new applicant accounts [12], key renewal with Shannon security AES [13], using multi authentication with Blowfish Algorithm, [14], RSA, AES [15] [18]. This research has not yet compared the performance of OTP encryption data. Therefore, this research will try to compare them.

2. Methodology

The research method begins with designing an OTP system, then evaluating it by looking at security performance and comparing the performance of the encryption algorithms of AES and Blowfish. Algorithm performance is measure by time speed. Time speed is a comparative parameter that aims to calculate the speed of the OTP encryption, decryption process and Avalanche effect.

3. Result and Discussion

Following the analysis of user needs in designing the OTP system, for the first time, the user registers the name, password, email, and cellphone number used to send OTP messages. Next, verify to activate the account and log in using the username and password when registering initially.

Before successfully logging in to the user page, the OTP insert menu will appear. Check the SMS from the cellphone that was register earlier. Enter the OTP code into the OTP Key insert menu. The system will validate the OTP code. This OTP is only used for one login. If successful, it will enter the application user page. When sending an OTP message on a public network, the message is encrypted using the Blowfish Algorithm and AES into an OTP key code. So that OTP messages are not stolen [16] by third parties or attacker.
Figure 2. OTP Application

In the testing of the application has been running well. When the web application is running, the user can enter a username and password on the login page. The system will perform user validation. If valid, the system will send an OTP code to the user via the mobile number registered in the database. Enter the OTP code on the Insert-OTP-Key menu display. If successful, the user will enter the user page (dashboard).

Furthermore, testing the performance of the encryption algorithm by comparing the AES and Blowfish algorithms [17]. The encryption algorithm's performance is shown in Figure 3 below.

![Figure 3](image)

Figure 3. Performance of Algorithm Encryption in OTP data

Figure 3 the performance of algorithm encryption in OTP data. Performance testing was conducted 30 times by looking at the speed aspect of the OTP message encryption process. The average encryption speed of the AES algorithm is 0.099735267 millisecond, and the Blowfish algorithm is 0.1151553 millisecond. From this value, it means that the AES algorithm is superior to the Blowfish algorithm in terms of encryption speed. As for the decryption shown in Figure 4 below.
Figure 4. Performance of Algorithm Decryption in OTP data

Figure 4 the performance of algorithm decryption in OTP data. Performance testing was carried out 30 times by looking at the speed aspect of the OTP message decryption process. The average decryption speed of the AES algorithm is 0.100144433 milliseconds, while the average decryption speed of the Blowfish algorithm is 0.145523033 milliseconds. From this value, it means that the AES algorithm is also superior to the Blowfish algorithm in terms of decryption speed.

Figure 5. Performance of the Avalanche effect in OTP data

Figure 5 performance of the avalanche effect in OTP data. The Avalanche effect is one of the comparative parameters used in determining the level of encryption algorithm security. The results of the encryption can be said to be good if one input bit produces changes in the output. Testing was done by looking at the comparison of changes in one character bit from two ciphertext inputs with a symmetrical key "password" as much as 30 times. The results obtained an average percentage of 37.45% for AES and 31.46% for Blowfish. From this percentage, it means that the AES algorithm is superior to the Blowfish algorithm in the avalanche effect comparison with a percentage difference of ± 6%.

4. Conclusion

One-Time Password (OTP) can increase the security of username and password data when logging into web applications. The OTP application implements the AES and Blowfish algorithms to encrypt the verification code. Verification code using an SMS gateway. Testing is done by looking at security
performance and comparing the encryption and decryption speed performance of Blowfish and AES algorithms. The results of the research design show that OTP is running well where the performance of the AES algorithm has advantages in terms of encryption and decryption speed compared to the Blowfish algorithm with a difference of ± 0.015 milliseconds for encryption and ± 0.04 milliseconds for decryption. The avalanche effect generated by the AES algorithm is superior to the Blowfish algorithm in the avalanche effect comparison with a percentage difference of ± 6%.

References
[1] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, “Communication network requirements for major smart grid applications in HAN, NAN and WAN,” *Comput. Networks*, vol. 67, pp. 74–88, 2014.
[2] W. Cheng et al., “Back to Business and (Re) employing Workers? Labor Market Activity During State COVID-19 Reopenings,” 2020.
[3] D. Aimeur, E., Schonfeld, “The ultimate invasion of privacy: Identity theft,” in *2011 Ninth Annual International Conference on Privacy, Security and Trust*, 2011, pp. 24–31.
[4] R. Rahim, N. Kurniasih, M. Mustamam, L. Andriany, U. Nasution, and A. H. Mu, “Combination Vigenere Cipher and One Time Pad for Data Security,” *Int. J. Eng. Technol.*, vol. 7, no. 2.3, pp. 92–94, 2018.
[5] D. G. Firesmith, “Security use cases,” *J. object Technol.*, vol. 2, no. 3, 2003.
[6] K. Renaud and V. Zimmermann, “Guidelines for ethical nudging in password authentication,” *SAIEE Africa Res. J.*, vol. 109, no. 2, pp. 102–118, 2018.
[7] D. E. Kurniawan, N. R. Hartadi, and P. Prasetyawan, “Analisis Hasil Teknik Penyembunyian Hak Cipta Menggunakan Transformasi DCT dan RSPPMC pada Jejaring Sosial.”
[8] J. M. Esparza, “Understanding the credential theft lifecycle,” *Comput. Fraud Secur.*, vol. 2019, no. 2, pp. 6–9, 2019.
[9] S. Glăvan, D., Răcuciu, C., Moinescu, R., Eftimie, “Sniffing attacks on computer networks,” *Sci. Bull. Mircea cel Batran’ Nav. Acad.*, vol. 23, no. 1, pp. 202A--207, 2020.
[10] F. Cheng, “A secure mobile OTP Token,” in *International Conference on Mobile Wireless Middleware, Operating Systems, and Applications*, 2010, pp. 3–16.
[11] J. Lee and A. C. C. Service, “A Secure Mobile OTP Authentication Scheme for User Mobility Cloud VDI Environment,” vol. 6, no. 10, pp. 774–777, 2012.
[12] E. P. Nugroho, R. R. J. Putra, and I. M. Ramadhan, “SMS authentication code generated by Advance Encryption Standard (AES) 256 bits modification algorithm and One time Password (OTP) to activate new applicant account,” in *2016 2nd International Conference on Science in Information Technology (ICSITech)*, 2016, pp. 175–180.
[13] P. V. Mankar, “Key updating for leakage resiliency with application to Shannon security OTP and AES modes of operation,” in *2017 International Conference on IoT and Application (ICIOT)*, 2017, pp. 1–4.
[14] A. R. L. Reyes, E. D. Festijo, and R. P. Medina, “Securing one time password (otp) for multifactor out-of-band authentication through a 128-bit blowfish algorithm,” *Int. J. Commun. Networks Inf. Secur.*, vol. 10, no. 1, pp. 242–247, 2018.
[15] G. Singh and M. Garg, “Enhanced Cloud Security using Hybrid Mechanism of RSA, AES and Blowfish Data Encryption with Secure OTP,” *Int. J. Comput. Technol.*, vol. 18, pp. 7364–7380, 2018.
[16] D. E. Kurniawan and N. Narupi, “Teknik Penyembunyian Data Menggunakan Kombinasi Kriptografi Rijndael dan Steganografi Least Significant Bit (LSB),” *J. Tek. Inform. dan Sist. Inf.*, vol. 2, no. 3, Oct. 2016, doi: 10.28932/jutisi.v2i3.487.
[17] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, “A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish,” *Procedia Comput. Sci.*, vol. 78, no. 1, pp. 617–624, 2016.