World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:14, No:01, 2020

Secure Automatic Key SMS Encryption Scheme Using Hybrid Cryptosystem: An Approach for One Time Password Security Enhancement

Authors : Pratama R. Yunia, Firmansyah, I., Ariani, Ulfa R. Maharani, Fikri M. Al

Abstract : Nowadays, notwithstanding that the role of SMS as a means of communication has been largely replaced by online applications such as WhatsApp, Telegram, and others, the fact that SMS is still used for certain and important communication needs is indisputable. Among them is for sending one time password (OTP) as an authentication media for various online applications ranging from chatting, shopping to online banking applications. However, the usage of SMS does not pretty much guarantee the security of transmitted messages. As a matter of fact, the transmitted messages between BTS is still in the form of plaintext, making it extremely vulnerable to eavesdropping, especially if the message is confidential, for instance, the OTP. One solution to overcome this problem is to use an SMS application which provides security services for each transmitted message. Responding to this problem, in this study, an automatic key SMS encryption scheme was designed as a means to secure SMS communication. The proposed scheme allows SMS sending, which is automatically encrypted with keys that are constantly changing (automatic key update), automatic key exchange, and automatic key generation. In terms of the security method, the proposed scheme applies cryptographic techniques with a hybrid cryptosystem mechanism. Proofing the proposed scheme, a client to client SMS encryption application was developed using Java platform with AES-256 as encryption algorithm, RSA-768 as public and private key generator and SHA-256 for message hashing function. The result of this study is a secure automatic key SMS encryption scheme using hybrid cryptosystem which can guarantee the security of every transmitted message, so as to become a reliable solution in sending confidential messages through SMS although it still has weaknesses in terms of processing time.

Keywords : encryption scheme, hybrid cryptosystem, one time password, SMS security
Conference Title : ICMAS 2020 : International Conference on Mobile Application Security
Conference Location : Bali, Indonesia
Conference Dates : January 13-14, 2020