Abstract

The number of threats on mobile devices increased by 261% by 2013.The factors that triggered an increase the number of threats was the increase in payment transactions using mobile payment. Attempts to these threats have been made, such as using the encryption method, Public Key Infrastructure (PKI) and the application of One Time Password on banking transactions. However, conventional method such as this cause problems in constrained device. The public key cryptosystem Identity Based Encryption - Elliptic Curve Cryptography (IBE-ECC) method has been proposed to overcome the weaknesses in the traditional method. IBE have a feature that can accept all String as a valid Public Key. IBE can simplify certificate management. However, only a few studies have tested IBE-ECC methods with other methods, such as IBE-RSA. There are a few research that implemented IBE-ECC methods in smartphone android. And the existing IBE-ECC is less than optimal in terms of running time and memory usage. Therefore, this research will designs the proposed IBE-ECC design and implements it on smartphone android and tests it with the IBE-RSA method. It is hoped that optimizing the multiplicative number of ECC points can made computing load to be ease and speed up the running time IBE-ECC system. The method used in this study is as follows: 1) Conducting literature study on IBE-ECC method, 2) Modifying the method, 3) Testing the performance of the proposed method with a comparison of existing methods and we analyzing the results. The performance of the proposed method in this final project is rated better, ie, an average of 5.5 % running time is faster than the IBE-ECC BF method and an average of 89.9 % Running time faster than the IBE-RSA method. In addition, the proposed method averaged more efficient use of Random Access Memory (RAM) 20.46 kB from IBE-ECC BF and 6287.46 kB from IBE-RSA. Purposed IBE-ECC has the same resistance to Bruteforce Attack with IBE-ECC BF and better 564 % than IBE-RSA method with the same private key.

Keywords: Encryption, ECC, RSA, IBE, Smartphone.