ABSTRAK

Penggunaan smart card dimulai pada tahun 1980 dan semenjak itu penggunaannya semakin meningkat. Namun, ada beberapa masalah terkait keamanan smart card seperti pemalsuan smart card, peniruan pengguna smart card, pencurian identitas smart card, dan penggunaan extract data smart card untuk menjebol skema autentikasi dari smart card. Untuk memperbaiki masalah pada smart card, autentikasi berdasarkan identitas dinamik diperkenalkan.

Lee et al [6] mengklaim bahwa skema milik mereka aman terhadap serangan peniruan pengguna smart card dan server spoofing. Namun, Li et al [7] mengklaim bahwa skema milik Lee masih rentan terhadap beberapa serangan seperti autentikasi yang jelek, dan terhadap serangan pemalsuan & server spoofing. Li et al [7] memperkenalkan sebuah skema baru untuk memperbaiki skema milik Lee dan mengklaim skemanya aman terhadap beberapa serangan seperti replay attack, forgery attack, server spoofing & registration centre spoofing attack, dan pencurian smart card. Wang et al [9] mengklaim bahwa skema milik Li rentan terhadap serangan offline password guessing, dan serangan DOS. Wang memperkenalkan sebuah skema baru yang aman terhadap serangan offline password guessing, pencurian verifikasi, peniruan pengguna, server masquerading attack, replay attack, parallel session attack, dan serangan DOS. Namun, Zhai et al [11] mengklaim bahwa skema milik Wang masih rentan terhadap serangan offline password guessing.

Research ini memperkenalkan sebuah skema baru untuk memperkuat skema milik Wang terhadap serangan offline password guessing. Skema baru menggunakan sebuah angka random u untuk mengamakan password user dan menggunakan sebuah timestamp untuk membuat nilai dinamis dari identitas pengguna. Skema baru telah terbukti lebih kuat dibanding skema milik Wang terhadap serangan offline password guessing. Probability keberhasilan dalam melakukan penebakan password pengguna adalah pangkat dua kalinya dari skema milik Wang. Skema yang baru juga telah terbukti sekuat skema milik Wang terhadap serangan user impersonation.

Kata kunci: autentikasi berdasarkan identitas dinamis; serangan offline password guessing.