PROTOKOL KEAMANAN ALTERNATIF UNTUK INTERAKSI PENGGUNA *LIVE CHAT* PADA *E-COMMERCE* BERBASIS WEB

ABSTRAK

Indonesia adalah salah satu pasar *e-commerce* terbesar di asia tenggara, sebanyak 5 juta jiwa melakukan transaksi di *e-commerce,* maka semakin banyak juga orang yang menggunakan layanan *live chat* untuk berkomunikasi dengan *customer service.* Dalam obrolan *live chat* seringkali *customer service* menanyai data lengkap *customer* seperti, nama lengkap, alamat, *e-mail¸* id transaksi dan lain lain, bertujuan untuk memverifikasi pembelian produk. Resiko yang akan terjadi salah satunya adalah *sniffing* yang akan berujung pada pencurian informasi rahasia yang akan menyebabkan kerugian besar terhadap *customer.* Oleh karena itu, diperlukan suatu tindakan untuk menghindari hal tersebut dengan membangun sebuah protokol keamanan alternatif untuk interaksi pengguna di *live chat* dengan menggunakan algorima kriptografi yang berguna untuk melindungi pesan yang bersifat rahasia. Cara untuk mempertahankan kerahasian (*Confidentiality*) dan integrasi data (*Data Integration*) yaitu dengan enkripsi dan fungsi hash. Algoritma yang dipakai adalah Rijndael 256 bits, RSA, dan SHA256. Tahapannya adalah pesan di enkripsi menggunakan Rijndael, kunci Rijndael dienkripsi oleh RSA, dan pesan akan dibangkitakan nilah hash nya menggunakan SHA256, hasil enkripsi dan nilai hash akan digabungkan dan dikirim kepada penerima. Untuk meningkatkan kompleksitas, algoritma Rijndael akan dimofikasi dibagian S-box dan ShiftRow berdasarkan kaidah prinsip *shannon,* hasil menunjukan semua lolos dalam uji *Randomness test,* tetapi modifikasi dibagian Shiftrow lebih menunjukan nilai *avalanche effect* yang lebih baik. Dengan begitu pesan akan sulit dicuri ataupun dirubah.

Kata Kunci : *Live Chat*, Kriptografi, Rijndael, RSA, SHA256

ALTERNATIVE SECURITY PROTOCOL FOR INTERACTIONS

LIVE CHAT USERS ON WEB-BASED E-COMMERCE

ABSTRACT

Indonesia is one of the biggest e-commerce market in southeast asia with approximately 5 million people do transactions in e-commerce. Then, many people use various features in e-commerce for doing transactions, such as live chat for communicating with customer service. In live chat, customer service always ask customers to request their complete transaction data which is confidential, and also personal data, such as name, address, e-mail, and so on to verify the data of purchased product. One of many risks that may happen at this feature is sniffing, that confidential data are vulnerable to be stolen and cause lost. Therefore, an action is needed to avoid that risk with developing an alternative security protocol by using cryptographic algorithms in live chat to protect contained confidential message. Method for protecting confidentiality and data integration is combination of Rijndael 256 bits and RSA encryption algorithm, and Hash function of SHA256. The first step of the used combination are original message is encrypted by Rijndael, then used keys by Rijndael is encrypted by RSA, and then hash value of original message will be resurrected by SHA256. Then, the final step is combining encrypted data result and hash value to be sent to receiver. To increase algorithm complexity, Rijndael will be modified in S-box and ShiftRow based on keys, the results represent modified algorithms pass Randomness Test, but modification in Shiftrow represent better avalanche effect value. Therefore, the message will be hard to be found or modified.

Keywords : *Live Chat*, Cryptography, Rijndael, RSA, SHA256