BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Keamanan jaringan menjadi aspek penting di era digital saat ini, dimana informasi seringkali dikirimkan melalui jaringan yang rentan terhadap berbagai serangan. Keamanan ini bertujuan untuk melindungi kerahasiaan, integritas, dan ketersediaan data yang dikirimkan melalui jaringan [1]. Salah satu komponen kunci keamanan jaringan adalah mekanisme distribusi kunci yang digunakan untuk memastikan komunikasi yang aman antara pihak-pihak yang berkomunikasi. Dalam konteks ini, protokol otentikasi seperti Needham-Schroeder dan Otway-Rees banyak digunakan dan telah dimodifikasi untuk meningkatkan efisiensi dan keamanan [2][3]. Namun, seiring kemajuan teknologi, kerentanan baru terhadap protokol-protokol tersebut terus ditemukan.

Distribusi kunci adalah elemen mendasar dari setiap sistem kriptografi. Ada dua jenis utama distribusi kunci: distribusi kunci simetris dan distribusi kunci asimetris. Distribusi kunci simetris menggunakan kunci yang sama untuk enkripsi dan dekripsi, sedangkan distribusi kunci asimetris menggunakan pasangan kunci publik dan kunci privat [4]. Sistem distribusi kunci ini sering kali berisiko mengalami koreksi kesalahan (*error correction*), terutama bila ada risiko data yang dikirimkan melalui jaringan rentan terhadap kehilangan atau diubah karena interferensi [5].

Modified Needham-Schroeder Protocol dan Otway-Rees Protocol adalah dua protokol autentikasi yang telah dimodifikasi untuk mengatasi beberapa kelemahan versi aslinya. Namun, kedua protokol tersebut masih menghadapi tantangan keamanan, seperti serangan *replay*, serangan *man-in-the-middle*, dan kebocoran informasi kunci [6][7]. Analisis keamanan terhadap protokol ini menggunakan logika Burrows-Abadi-Needham (BAN) telah menjadi pendekatan yang populer untuk mengidentifikasi kelemahan desain dan memberikan solusi perbaikan [8].

Logika BAN memungkinkan evaluasi formal terhadap asumsi keamanan yang digunakan dalam protokol autentikasi. Dengan menggunakan logika ini, dimungkinkan untuk menentukan apakah protokol benar-benar dapat menjamin

komunikasi yang aman dalam situasi yang kompleks [9][10]. Analisis ini sangat relevan dalam konteks protokol *Modified* Needham-Schroeder dan Otway-Rees, karena biasanya digunakan dalam berbagai aplikasi jaringan yang memerlukan tingkat keamanan tinggi [11].

Dalam konteks pendistribusian kunci, penggunaan kunci simetris dan asimetris mempunyai kelebihan dan kekurangan tersendiri. Distribusi kunci simetris cenderung lebih cepat tetapi rentan terhadap serangan jika kunci tidak diamankan dengan baik [12]. Di sisi lain, distribusi kunci asimetris memberikan keamanan yang lebih tinggi tetapi memerlukan komputasi yang besar. Kombinasi keduanya sering digunakan dalam praktik untuk mengoptimalkan efisiensi dan keamanan [13]. Namun, kelemahan desain dalam protokol otentikasi dapat menyebabkan kegagalan sistem bahkan ketika metode distribusi kunci yang kuat digunakan [14].

1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian ini adalah:

1. Apa kelemahan keamanan yang ada dalam protokol *Modified* Needham-Schroeder dan Otway-Rees?
2. Apa rekomendasi perbaikan untuk meningkatkan keamanan protokol *Modified* Needham-Schroeder dan Otway-Rees?

1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah:

1. Analisis dibatasi hanya pada protokol *Modified* Needham-Schroeder dan Otway-Rees, tanpa memasukkan protokol lain.
2. Fokus pada aspek keamanan yang dapat dievaluasi dengan logika BAN.

1.4 TUJUAN

Tujuan dari penelitian ini adalah:

1. Mengidentifikasi kerentanan dari keamanan Protokol *Modified* Needham-Schroeder dan Otway-Rees.
2. Mengidentifikasi kelemahan dan kekurangan dari protokol *Modified* Needham-Schroeder dan Otway-Rees.

1.5 MANFAAT

Penelitian ini diharapkan dapat memberikan gambaran tentang meningkatkan keamanan protokol *Modified* Needham-Schroeder dan Otway-Rees. Dengan membantu dalam mengidentifikasi dan mencatat potensi kerentanan yang ada dalam protokol tersebut, memverifikasi protokol *Modified* Needham-Schroeder dan Otway-Rees mematuhi prinsip-prinsip keamanan dasar autentikasi dan kerahasiaan, serta menilai efektivitas modifikasi yang telah dilakukan untuk meningkatkan keamanannya.

1.6 SISTEMATIKA PENULISAN

Penelitian ini dibagi dari beberapa bab. Bab 1 berisi tentang latar belakang, rumusan masalah, tujuan, manfaat penelitian, batasan masalah dan sistematika penulisan. Bab 2 membahas tentang kajian pustaka serta dasar teori yang berisi mengenai konsep *Security Attack*, BAN *Logic*, *protocol analysis, symmetric key distribution*, *public key distribution*, *public key encryption* dan *key establishment protocols*. Pada bab 3 berisi tentang alat yang digunakan dan alur penelitian. Dalam bab 4, membahas tentang rancangan sistem, hasil analisa menggunakan logika BAN. Pada bab 5 berisikan tentang kesimpulan dan saran dari hasil perancangan sistem dan hasil analisa yang telah dilakukan.