REQUIREMENT ENGINEERING SISTEM KRIPTOGRAFI *RSA* PADA *GMAIL*

Novanto Prio Utomo [1)], **Tining Haryanti**[2)]

[1), 2)] *Program Studi Teknik Komputer, Fakultas Teknik, Universitas Muhammadiyah Surabaya*
Jl Sutorejo No. 59, Surabaya
Email : novantopu@gmail.com[1)], tiningharyanti@ft.um-surabaya.ac.id[2)]

Abstrak

Dalam tahun 2022 kemarin di Indonesia menurut BSSN terjadi kasus cybercrime sebanyak 714.170.967 kasus yang dialamai oleh perorangan maupun organisasi mulai dari malware sampai kebocoran data atau informasi. Diantara banyaknya kasus cybercrime yang ada cabang terbesar yang sering terjadi kasus cybercrime adalah pada email. Penggunaan email yang paling sering digunakan di Indonesia adlah gmail dengan pengguna sebanyak 81,8 juta pengguna. Oleh karena itu dibutuhkanlah sebuah sistem keamanan yang baik untuk mengamankan data yang ada dalam email tersebut, salah satu metode untuk meningkatkan keamanan yang ada dalam penggunaan gmail adalah dengan metode kriptografi, dari sekian banyaknya metode kriptografi yang ada penggunaan kriptografi RSA dinilai lebih baik dalam mengamankan data dikarenakan kriptografi RSA memiliki kemampuan double key yakni public key dan private key untuk megamankan data yang ada. Untuk itu dalam penelitian ini penulis akan membuat sebuah dokumentasi requirement yang akan digunakan sebagai acuan dalam membuat Aplikasi Secure Email.

Kata kunci: *Cybercrime, Kriptografi, Kriptografi RSA, Requirement*

Abstract

In 2022, according to BSSN, in Indonesia there were 714,170,967 cybercrime cases experienced by individuals and organizations ranging from malware to data or information leaks. Among the many cybercrime cases, the biggest branch where cybercrime cases often occur is email. The most frequently used email in Indonesia is Gmail with 81.8 million users. Therefore, a good security system is needed to secure the data contained in the email. One method to increase the security that exists when using Gmail is the cryptographic method. Of the many existing cryptographic methods, the use of RSA cryptography is considered better in securing data. because RSA cryptography has double key capabilities, namely a public key and a private key to secure existing data. For this reason, in this research the author will create a requirements documentation that will be used as a reference in creating a Secure Email Application.

Keywords : *Cybercrime, Cryptography, RSA Cryptography, Requirements*

1. Pendahuluan

Perkembangan teknologi yang semakin pesat tidak dapat dipungkiri telah mengubah cara kerja berbagai kegiatan dalam bidang kehidupan manusia mulai dari perusahaan sampai pemerintah. Dengan perkembangan teknologi saat ini pertukaran informasi antar pihak sangat diperlukan. Jika keamanan pertukaran informasi tidak bisa di jaga, maka pihak lain dapat memanfaatkan informasi tersebut sehingga akan merugikan pihak-pihak yang berhak atas informasi tersebut. Pada masa kini pertukaran informasi menjadi lebih cepat dan mudah sebagaimana percakapan yang seharusnya tidak bisa dilakukan karena jarak yang jauh menjadi mungkin dengan email dan aplikasi chatingan yang lain, akan tetapi dengan mudahnya pertukaran informasi ini membuat banyak penggunanya lalai dalam keamanan data/informasi yang dilakukan waktu pertukaran informasi yang memungkinkan terjadinya resiko pencurian data [1].

Menurut data perusahaan keamanan siber Surfshark. Indonesia menempati urutan ke-5 negara dengan jumlah kasus kebocoran data terbanyak di dunia. Tercatat, ada 14,74 juta akun yang menglami kebocoran data di Indonesia selama kuartal III-2022 yang tercatat hingga 13 september 2022 [2]. Dari data tersebut diketahui bahwa di Indonesia masih banyak terjadi kasus kebocoran data yang merugikan banyak pengguna internet di Indonesia. Hal ini dapat menyebabkan kerusakan bagi individu ataupun organisasi tergantung dari data yang dicuri akan digunakan untuk apa oleh sipelaku. Dikarenakan itu perlu sebuah keamanan data yang kuat untuk mencegah hal-hal seperti kebocoran data terjadi.

Oleh sebab itu dalam peneitian ini penulis ingin membuat dokumentasi *requirement* yang diperlukan untuk membuat aplikasi secure email. Dokumentasi *requirement* ini merupakan tahapan yang krusial dalam pembuatan sebuah sistem dikarenakan pada tahapan ini akan menghasilkan *user requirement* yang berguna untuk memahami kebutuhan user dan menganalisisnya untuk pengembangan produk perangkat lunak [3]. Melihat pentingnya tahapan requirement engineering, perumusan masalah penelitian ini adalah bagaimana melakukan proses requirement engineering yang menjadi dasar bagi pembangunan aplikasi secure email. Penelitian ini dilakukan dengan tujuan untuk mengeksplorasi kebutuhan melalui proses Requirement Engineering.

2. Dasar teori

2.1 Kriptografi

kriptografi memiliki tiga fungsi dasar, yaitu: Enkripsi, Dekripsi, dan Kunci [4]. Enkripsi merupakan keamanan data yang dikirim agar tetap terjaga rahasia, dimulai dari pesan asli yang kemudian dirubah menjadi kode-kode yang tidak bisa dipahami. Dekripsi merupakan kebalikan dari enkripsi, yaitu proses pengembalian pesan yang sudah terenkripsi Kembali menjadi bentuk aslinya. Kunci yang dimaksud adalah kunci yang akan digunakan untuk melakukan enkripsi dan dekripsi, kunci terbagi menjadi dua, yaitu: kunci public (public key) dan kunci rahasia (private key) [5].

2.2 Kriptografi RSA

Algoritma RSA dibuat oleh tiga orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1977. Algoritma ini memiliki tiga tahapan utama, yaitu: pembangkitan kunci, enkripsi, dan dekripsi. Algoritma ini menerapkan kriptografi asimetris, yaitu kriptografi yang menggunakan dua jenis kunci yang berbeda: kunci publik dan kunci pribadi. Algoritma ini adalah yang pertama kali diketahui paling cocok untuk enkripsi, keunggulan utama dari algoritma ini adalah sulitnya memfaktorkan bilangan yang menjadi factor-faktor prima [6]. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin.

2.3 Requirement

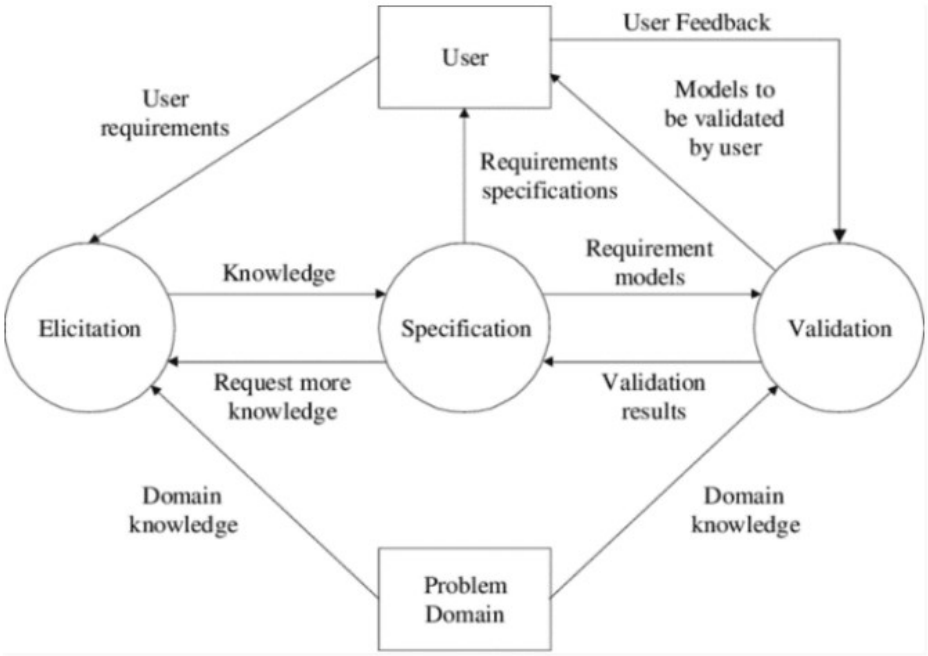
Requirements engineering adalah cabang dari software engineering yang mengurusi masalah yang berhubungan dengan: tujuan (dunia nyata), fungsi, dan batasan-batasan pada sistem software. Termasuk hubungan faktor-faktor tersebut dalam menetapkan spesifikasi yang tepat dari suatu software, proses evolusinya baik berhubungan dengan masalah waktu maupun dengan software lain (dalam satu famili) [7].

2.4 Requirement Engineering

Requirements engineering adalah cabang dari software engineering yang mengurusi masalah yang berhubungan dengan: tujuan (dunia nyata), fungsi, dan batasan-batasan pada sistem software. Termasuk hubungan faktor-faktor tersebut dalam menetapkan spesifikasi yang tepat dari suatu software, proses evolusinya baik berhubungan dengan masalah waktu maupun dengan software lain (dalam satu famili) [7].

3. Metodologi Penelitian

Metode yang digunakan dalam penelitian ini adalah menggunakan model *Iterative Requirement Engineering* yang dikembangkan oleh Loucopoulos dan Karakostas Seperti yang ditunjukan pada Gambar 1.



Gambar 1. *Loucopoulos and Karakostas model*

Pada Gambar 1. terdapat pemenuhan kebutuhan yang melibatkan beberapa tahpan penting yaitu:

A. Elicitation

Pada proses pertama yaitu elicitation memiliki aktivitas utama untuk mengumpulkan data dari pihak yang terkait. Dalam proses ini akan menghasilkan identifikasi masalah, perumusan kendala sistem, dan kendala sistem [8]. Pada tahapan ini terdapat dua aspek yaitu problem domain yang berarti area permasalahan yang harus disesuaikan dengan sistem perangkat lunak, dan terdapat User yang menjadi stakeholder dalam pengembangan system.

B. Specification

Pada tahap kedua yaitu specification dilakukan pemeriksaan pada kelengkapan, konsistensi serta tingkat kelayakan persyaratan. Pada tahap ini juga dilakukan analisis terkait proses bisnis, serta pihak terkait dengan merancang diagram use case diagram, activity diagram, class diagram, arsitektur sistem dalam perancangan architecture models.

C. Validation

Pada tahap validation dilakukan dengan menggunakan prototyping, dikarenakan protoyping memiliki keuntungan dalam hal komunikasi yang intens antara pengguna dan pengembang [9].

4. Pengujian dan Pembahasan

A. Elicitation

Pada tahap elicitation ini, identifikasi masalah dilakukan dengan studi literatur tentang data kebutuhan terkait pengembangan Aplikasi Secure Email. Dari data yang didapatkan dilakukan eksplorasi dan perumusan alternatif solusi seperti terlihat pada Tabel 1.

Tabel 1. *EKSPLORATIF ALTERNATIF SOLUSI*

No	Tujuan	Kebutuhan	Solusi
1.	Mengakomodasi user untuk mengamankan data pada gmail	Sebuah platform untuk mengamankan data pada gmail	Mengembangkan sebuah platform untuk mengamankan data pada gmail

2.	Mempermudah pengaksesan sistem dengan platform berbasis web	Platform yang mudah diakses	Mengembangkan platform berbasis web, untuk mempermudah user dalam mengakses platform

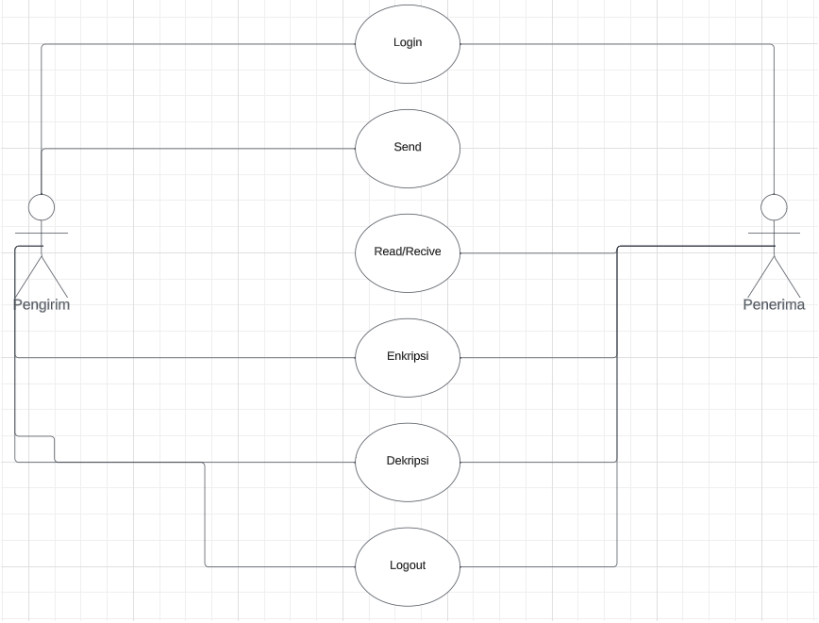
Solusi yang didefinisikan pada Tabel 1 merupakan dasar dari pembuatan aplikasi secure email, kebutuhan fungsional serta persyaratan fungsional aplikasi secure email ditunjukkan pada Tabel 2.

Tabel 2. *DEFINISI KEBUTUHAN FUNGSIONAL SISTEM*

No	Kebutuhan	Fitur
1	User dapat membuat, mengirim pesan	Form Tulis Pesan
2	User dapat membuat kunci saat mengirim pesan	Form Tulis Pesan dengan kunci
3	User dapat melihat pesan yang sudah terkirim	Dashbord Kontak Masuk

B. Specification

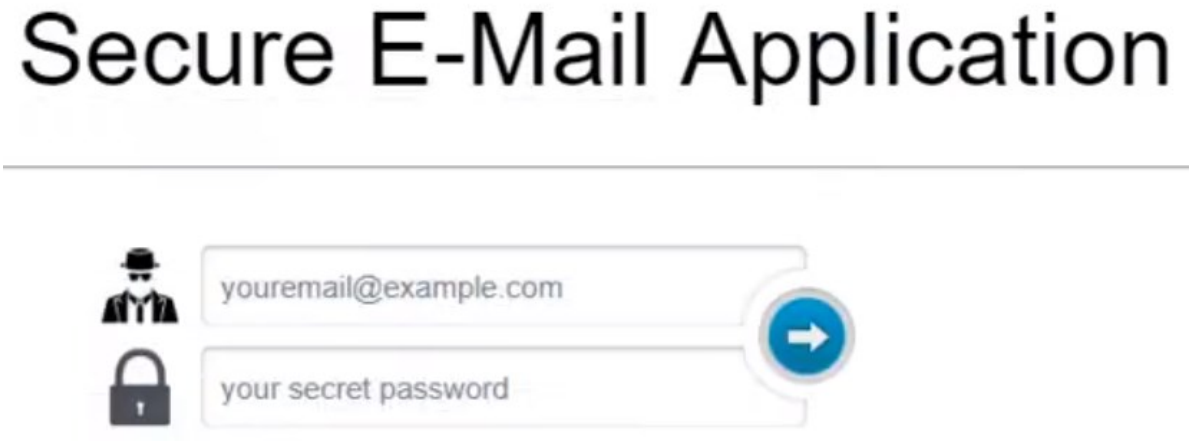
Pada tahapan specification, kebutuhan fungsional diterjemahkan ke dalam Unified Modeling Language (UML) untuk membantu menyelesaikan permasalahan tersebut, maka dilakukan eksplorasi dan perumusan alternatif solusi [10]. Use case diagram Aplikasi Secure Email ditunjukkan pada Gambar 2.



Gambar 2. *Use case Diagram Aplikasi Secure Email*

C. Validation

Tahap validasi dilakukan dengan menggunakan metode prototyping yang merupakan bentuk visualisasi solusi [11], sehingga stakeholder dapat memastikan bahwa solusi yang dirancang sesuai dengan kebutuhan pengguna. Mockup dari aplikasi secure email dapat dilihat pada Gambar 3., 4., 5. dan 6.

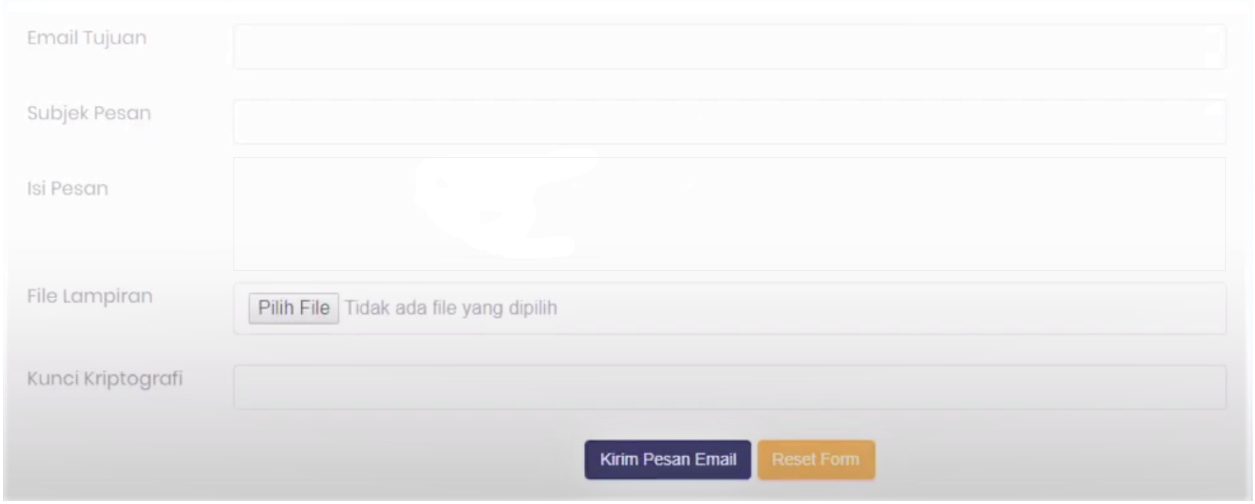


Gambar 3. *Mockup* Login User

Pada Gambar3 Adalah halaman awal dimana user akan diminta untuk melakukan login dengan menggunakan gmailnya. Setelah user melakukan login user akan dipindahkan ke laman dashboard yang tertera pada Gambar 4

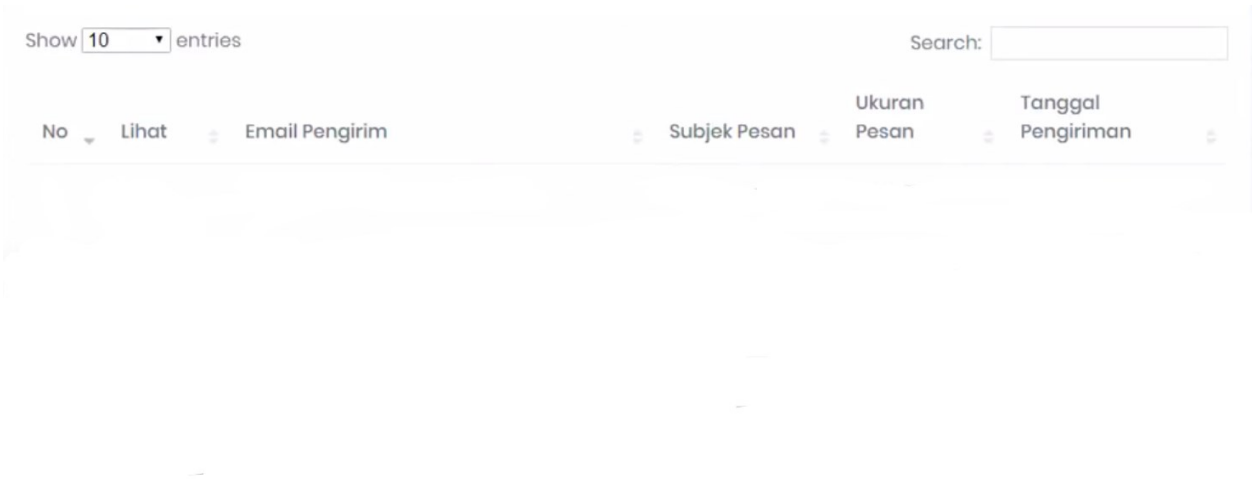
Gambar 4. *Mockup Dashboard Aplikasi Secure Email*

Pada Gambar 4. Ini adalah laman menu utama dari aplikasi secure email. Pada dashboard aplikasi secure meail terdapat beberapa menu yaitu: Tulis pesan, Kontak masuk, Bantuan, Tentang, dan Logout.



Gambar 5. *Mockup form Tulis Pesan*

Pada Gambar 5. Merupakan form dari menu tulis pesan yang berisikan email tujuan yang hendak dikirm, subjek pesan atau judul pesan yang ingin dikirim, isi pesan, file lampiran, dan kunci kriptografi yang akan digunakan untuk mengamankan pesan.



Gambar 6. *Mockup Dashboard Kontak Masuk*

Pada Gambar 6. Merupakan tampilan dari menu kontak masuk dimana dalam menu kontak masuk ini user dapat melihat pesan-pesan yang diterima, pesan akan ditampilkan kedalam 10 row tabel, user juga dapat mencari pesan dengan menggunakan fitur search dengan cara memasukkan kata kunci dari pesan yang ingin dicari.

5. Kesimpulan

Rekayasa kebutuhan yang dilakukan mengungkap detail permasalahan serta kebutuhan untuk membantu user pengguna gmail dalam mengamankan pesan. Berdasarkan eksplorasi solusi alternatif, model sistem yang dihasilkan dapat digunakan sebagai panduan atau blue print untuk pengembangan aplikasi Secure Email Aplication.

Daftar Pustaka

[1] H. a. H. H. F. Syaputra, "APLIKASI ENKRIPSI DATA PADA FILE TEKS DENGAN ALGORITMA RSA (RIVEST SHAMIR ADLEMAN)," *Semantik,* 2012.

[2] Surfshark, "Data breach statistics 2021 vs. 2022," 18 Januari 2023. [Online]. Available: https://surfshark.com.

[3] N. S. D. H. B. Y. A. S. Hanusia Manuel Oktrivania Zamili, "REQUIREMENT ENGINEERING APLIKASI PENGELOLAAN PROSES PERTANIAN PADA KOMUNITAS TANI MENGGUNAKAN LOUCOPOULOS DAN KARAKOSTAS ITERATIVE MODEL," *Jurnal Ilmiah Penelitian dan Pembelajaran Informatika (JIPI),* 2023.

[4] O. K. W. NUNIEK FAHRIANI, "CRYPTOGRAPHY ON AUDIO FILES USING THE BLOWFISH," *Journal of Electrical Engineering and Computer Sciences,* 2018.

[5] D. Ariyus, Pengantar Ilmu Kriptografi : teori analisis & implementasi, Yogyakarta: Penerbit Andi, 2018.

[6] H. F. H. Hendri Syaputra, "APLIKASI ENKRIPSI DATA PADA FILE TEKS DENGAN ALGORITMA RSA," *Semantik,* 2012.

[7] P. Zave, "Classification of research efforts in requirements engineering," *IEEE International Requirements Engineering Conference,* 1995.

[8] S. M. Nagy Ramadan, "Requirements Engineering in Scrum Framework," *International Journal of Computer Applications,* 2016.

[9] D. W. U. Egia Rosi Subhiyakto, "ANALISIS DAN PERANCANGAN APLIKASI PEMODELAN KEBUTUHAN PERANGKAT LUNAK MENGGUNAKAN METODE PROTOTYPING," *Seminar Nasional Multi Disiplin Ilmu Unisbank,* 2017.

[10] P. M. Brilyan Hendra Suryawan, "RANCANGAN STANDAR OPERASIONAL PROSEDUR (SOP) REQUIREMENT ENGINEERING MENGGUNAKAN SOFT SYSTEM METHODOLOGY," *Syntax Idea,* 2021.

[11] R. A. A. E. Fikri Maulana, "Aplikasi Manajemen Laboratorium Menggunakan Metode MVVM Berbasis Android," *Jurnal Ilmiah Teknologi Sistem Informasi,* 2022.