JISKa, Vol. 4, No. 3, JANUARI, 2020, Pp. 12 – 17
ISSN : 2527 – 5836 (print) | 2528 – 0074 (online)

Pengembangan Aplikasi *Computer Based Test* dengan Protokol *Two Central Facilities*

Muhammad Nasyithul Ibad [(1)], Syarif Alqoroni [(2)],
Muhammad Ammarullah Ridho [(3)] Khadijah Fahmi Hayati Holle[(4)]
Jurusan Teknik Informatika – UIN Maulana Malik Ibrahim Malang
JL. Gajayana No. 50, Dinoyo, Kec. Lowokwaru, Kota Malang - Indonesia
e-mail : muhammad.nasyithul.ibad@gmail.com[(1)], syarifalqoroni2@gmail.com[(2)],
study.ammar@gmail.com[(3)] khadijah.holle@uin-malang.ac.id[(4)]

Abstract

The Indonesian government has issued a policy on Ujian Nasional Berbasis Komputer (UNBK), or it can be called CBT (Computer Based Test). In this study is the development of the CBT system using the Two Central Facilities protocol, which consists of the Central Legitimization Agency (CLA) and the Central Tabulating Facilities (CTF). In developing this CBT system, CLA is used to authenticate the examinees, while CTF is used to provide questions and calculation of exam answers. To maintain security added encryption using the RSA Algorithm (Rivest-Shamir-Adleman) which functions to convert data into ciphertext. From the results of functional trials, this system has succeeded in applying the Two Central Facilities protocol. This system has been connected to the CLA and CTF servers and all data has been successfully encrypted. For this reason, in the future schools will be endeavored to implement the development of the CBT system to avoid fraud.

Keywords : UNBK, Two Central Facilities, RSA Encryption

Abstrak

Ujian Nasional merupakan suatu ujian yang menjadi tolak ukur pemahaman dari seorang siswa, akan tetapi Ujian Nasional secara tertulis rawan terjadinya berbagai kecurangan. Oleh karena itu pemerintah mengeluarkan kebijakan tentang Ujian Nasional Berbasis Komputer (UNBK) atau bisa disebut CBT (Computer Based Test). Dalam penelitian ini merupakan pengembangan sistem CBT dengan menggunakan protokol *Two Central Facilities*, yang terdiri dari *Central Legitimization Agency* (CLA) dan *Central Tabulating Facilities* (CTF). Dalam pengembangan sistem CBT ini, CLA digunakan untuk autentikasi peserta ujian, sedangkan CTF digunakan untuk penyedia soal dan perhitungan jawaban ujian. Untuk menjaga keamanan ditambahkan enkripsi menggunakan Algoritma RSA (*Rivest-Shamir-Adleman*) yang berfungsi untuk merubah data menjadi cipherteks. Dari hasil uji coba fungsional, pada sistem ini telah berhasil dalam menerapkan protokol Two Central Facilities. Sistem ini telah terhubung dengan server CLA dan CTF serta semua data telah berhasil terenkripsi menggunakan Algoritma RSA, sehingga semua terjamin keamananya. Untuk itu, kedepannya sekolah-sekolah diusahakan menerapkan hasil pengembangan sistem CBT ini.

Kata Kunci : UNBK, Two Central Facilities, Enkripsi RSA

1. PENDAHULUAN

Berkembangnya teknologi menjadikan banyak proses yang beralih ke media digital dan komputerisasi, banyak pekerjaan yang awalnya dikerjakan oleh manusia mulai tergantikan oleh mesin dan komputer. Fenomena ini terjadi di berbagai sektor kehidupan. Salah satu perubahan yang terjadi yaitu di bidang pendidikan. Perubahan yang kita ketahui yakni bergantinya Ujian Nasional (UN) berbasis ujian tulis menjadi Ujian Nasional Berbasis Komputer (UNBK) atau lebih umum dikenal dengan istilah CBT (*Computer Based Test*).

UNBK pertama kali diselenggarakan pada tahun 2014 secara online dan dibatasi di SMP Indonesia Singapura dan SMP Indonesia Kuala Lumpur (SIKL). Hasil dari penyelenggaraan UNBK pada kedua sekolah tersebut menghasilkan nilai yang memuaskan, sehingga mendorong untuk meningkatkan pengetahuan siswa terhadap Teknologi Informasi dan Komunikasi (TIK). (Kemendikbud, 2019)

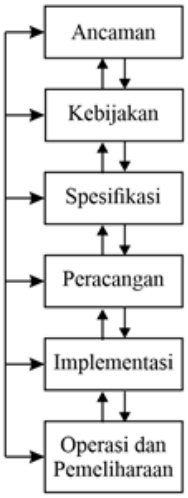
Laporan dan hasil CBT lebih cepat diolah, namun berbagai kecurangan tidak akan terhindarkan pada sistem UNBK (Poggio, Glassnapp, & Yang, 2005). Oleh karena itu sistem UNBK yang dibuat harus memenuhi standar untuk menjamin keamanan pada setiap ancaman yang akan terjadi. Menurut pendapat Bruce Schneir (1996), salah satu solusi dalam menjaga keamanan data adalah dengan adanya protokol *Two Central Facilities* yang terdiri dari *Central Legitimization Agen* (CLA) untuk autentikasi user dan *Central Tabulating Facilities* untuk perhitungan data Schneir, 1996). Siressha dan Chackai (2005) pada bukunya *Secure Virtual Election Booth with Two Central Facilities*, juga memaparkan desain protokol *Secure Election* dengan *Two Central Facilities*, yaitu *Central Legitimization Agency* (CLA) dan *Central Tabulating Facilities* (CTF).

Selain itu aspek keamanan pada *Two Central Facilities* dapat dicapai dengan menggunakan algoritma kriptografi, menerapkan konsep dengan menyembunyikan informasi, dan menerapkan protokol keamanan. Kriptografi digunakan untuk menjaga pesan dari pihak yang tidak memiliki hak untuk mengakses suatu informasi. Kerahasiaan dapat dicapai dengan menggunakan ukuran keamanan algoritma fisik atau matematika (Firdaus, Wahyudin, & Nugroho, 2017).

Salah satu alasan algoritma RSA (*Rivest—Shamir—Adleman*) paling banyak digunakan untuk kriptografi adalah karena memungkinkan salah satu dari dua kunci untuk mengenkripsi pesan dan kunci yang berlawanan untuk mendekripsi, sehingga menjanjikan kerahasiaan, integritas, keaslian, dan non-reputasi data dan komunikasi elektronik (Nisha & Farik, 2017). Dalam algoritma RSA, satu pihak menggunakan kunci publik dan pihak lain menggunakan kunci rahasia, yang dikenal sebagai kunci pribadi (Saranya, Vinothini, & Vasumathi, 2014).

2. METODE PENELITIAN

Penelitian ini menggunakan metode *Security Life Cycle*. Terdapat-tahapan tahapan utama yang diciptakan dalam *Security Life Cycle* (Bishop, 2003).



Gambar 1. Security life cycle

1) Ancaman (*Threats*)
Sistem *Computer Based Test* diharapkan mampu melindungi sistem dari berbagai ancaman yang mungkin terjadi. Contoh dari ancaman ini antara lain :
   - Modifikasi identitas
     Yakni ancaman perubahan data-data yang ada di server seperti pengubahan nama, NISN dan data diri lainnya
   - Penyamaran
     Yakni ancaman yang berupa peniruan suatu entitas terhadap entitas yang lain, entitas disini sebagai peserta ujian.
   - Disruption

Yakni penyerangan terhadap sistem, penyerangan ini melemahkan sumber daya sistem sehingga tidak dapat diakses atau sistem mengalami crash. (Muharram & Satrya, 2015)

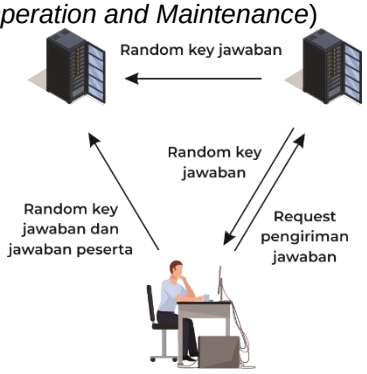
2) Kebijakan (*Policy*)
Keamanan CBT ini dibagun secara komputerisasi dan dapat digunakan apabila terdapat dua aturan yakni privasi siswa dan pencegahan terhadap kecurangan. Dalam suatu aturan yang aman harus memiliki beberapa persyaratan antara lain:
- Hanya peserta ujian yang dapat mengerjakan ujian CBT atau login atau autentikasi
- Peserta tidak bisa memilih lebih dari satu jawaban
- Peserta tidak boleh menggantikan atau digantikan oleh orang lain.
- Peserta boleh memastikan kembali identitas atau jawaban yang terisi sebelum selesai ujian.

3) Spesifikasi (*Specification*)
Pada sistem ini terdiri dari dua server yaitu server CLA, server CTF. Server CLA akan mengautentikasi siswa menggunakan NISN dan password. Sedangkan server CTF menyediakan soal yang akan dikerjakan oleh peserta ujian. CTF bertindak dalam pengumpulan ja\waban peserta ujian dan menghitung jawaban yang benar. Seluruh data akan tersimpan secara cipherteks menggunakan algoritma RSA, sehingga keamanan informasi lebih terjaga. Secara umum, sistem yang dibangun haruslah memberikan jaminan bahwa informasi yang diakses pengguna tidak diganggu oleh pihak pihak yang tidak berwenang dalam mengakses sistem, namun tetap mempertimbangkan sisi kecepatan pertukaran data. Pengiriman data dalam setiap proses, misalnya registrasi juga haruslah terjamin keamanannya sehingga diperlukan pengenkripsian data sebelum pengiriman dilakukan.

4) Perancangan (*Design*)
Pada sistem ini dibagi menjadi dua bagian, yaitu perancangan sistem secara umum yang membahas keseluruhan sistem yang dibagun menggunakan protokol *Two Central Facilities* yang telah dimodifikasi. Dalam melakukan perancangan server CLA dan CTF, serta penggunaan algoritma RSA perlu diketahui bahwa penggunaan setiap server. Selain itu perlu penentuan hardware yang sesuai dengan kebutuhan sistem.

5) Implementasi (*Implementation*)
Sistem CBT idealnya adalah suatu perangkat yang dirakit untuk menjadi sistem ujian berbasis online atau yang biasa dikenal dengan CBT dengan kebijakan sebagai berikut :
- Peserta atau siswa disediakan keyboard, mouse dan headphone untuk memudahkan siswa mengerjakan soal-soal yang diujikan.
- Siswa hanya berinteraksi dengan sistem CBT menggunakan perangkat yang telah disediakan panitia ujian.

6) Operasi dan Pemeliharaan (*Operation and Maintenance*)



Gambar 2. Skema Protokol Two Central Facilities

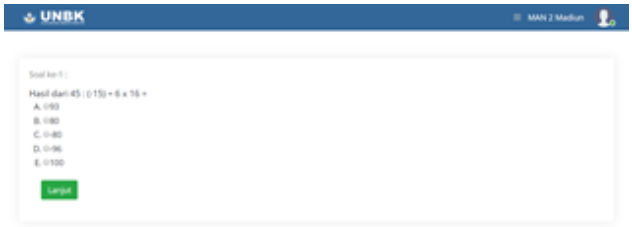
3. HASIL DAN PEMBAHASAN

4. Hasil Implementasi

Implementasi *Two Central Facilities* pada UNBK yaitu dalam penggunaan *Central Legitimization Agency* (CLA) sebagai autentikasi siswa dan *Central Tabulating Facilities* (CTF) sebagai perhitungan hasil jawaban peserta. Pada sistem ini terdapat tiga komponen diantaranya tampilan user, server CLA dan server CTF. Tampilan user merupakan komponen untuk peserta agar dapat berinteraksi dengan sistem, sehingga peserta dapat mengerjakan soal-soal CBT. CLA merupakan pusat data yang berfungsi dalam penyimpanan data siswa. Data tersebut tidak dapat dilihat orang lain termasuk pihak *Central Tabulating Facilities* (CTF). Data yang ada di *Central Legitimization Agency* (CLA) digunakan untuk login dan autentikasi. Sedangkan *Central Tabulating Facilities* (CTF) merupakan komponen kedua yang ada di sistem ini dan berfungsi untuk penyedia soal dan perhitungan nilai dari jawaban siswa.

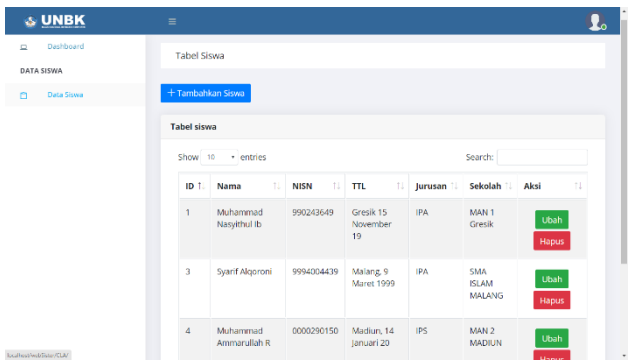
Gambar 3. Halaman autentikasi siswa

Gambar 3 merupakan tampilan di halaman pertama yakni form login peserta ujian UNBK. Gambar tersebut mempunyai inputan User ID berupa NISN dan password, kedua form tersebut sebagai fungsi autentikasi peserta di sistem CBT.



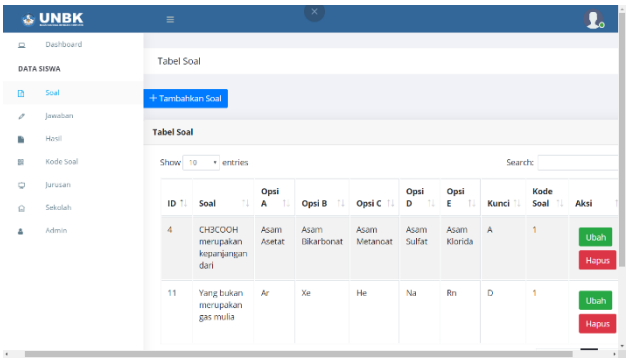
Gambar 4. Tampilan UNBK

Gambar 4 merupakan tampilan UNBK yang berisi tentang soal dan opsi jawaban yang akan dikerjakan oleh peserta ujian. Soal yang telah dikerjakan semuanya akan dikirimkan ke server CTF yang akan dihitung hasil ujiannya.

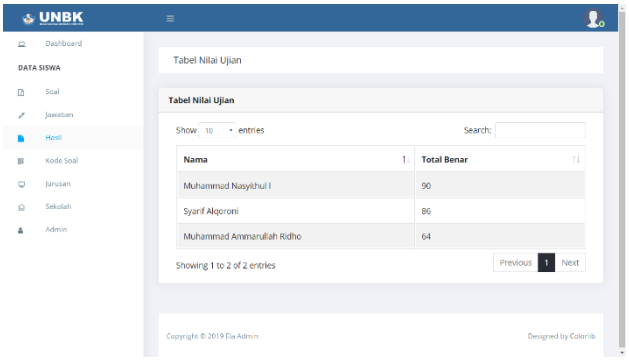


Gambar 5. Tampilan Data Siswa pada CLA

Tampilan dashboard pada Gambar 5 digunakan admin untuk menginputkan data siswa sebagai peserta ujian. Data yang diinputkan berupa nama, NISN, TTL, jurusan, dan asal sekolah.

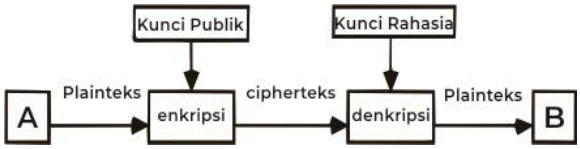


Gambar 6. **Tampilan Data Soal pada CTF**



Gambar 7. **Tampilan Hasil penilaian pada CTF**

Gambar 6 merupakan tampilan tabel soal yang digunakan admin untuk menginputkan data soal beserta kunci jawaban. Sedangkan pada Gambar 7 merupakan hasil yang telah dilakukan setelah pencocokan jawaban siswa dengan kunci jawaban.



Gambar 8. Skema algoritma RSA

Gambar 8 menjelaskan tentang proses enkripsi dengan algoritma RSA menggunakan sebuah kunci publik sehingga menghasilkan suatu chiperteks. Sedangkan proses dekripsi menggunakan kunci rahasia yang disediakan oleh server.

5. Uji Fungsionalitas
Uji fungsional diterapkan pada manajemen data siswa pada CLA, manajemen data soal pada CTF dan tampilan pengerjaan ujian.

Tabel 1. Hasil pengujian fungsional sistem

Skenario Pengujian	Hasil
Penginputan data siswa pada server CLA	Berhasil
Semua data telah terenkripsi pada server CLA	Berhasil
Penginputan data siswa pada server CTF	Berhasil
Semua data telah terenkripsi pada server CTF	Berhasil
Perangkat ujian mengambil data dari CLA dan CTF	Berhasil
Server CTF dapat menghitung hasil ujian peserta	Berhasil

Berdasarkan Tabel 1, perangkat ujian dapat mengambil data siswa sebagai autentikasi user dari server CLA dan mengambil data soal pada server CTF serta mengirimkan hasil jawaban ke server CTF. Server CTF telah berhasil dalam perhitungan hasil ujian.

Gambar 9. Data yang telah dienkripsi dengan Algoritma RSA

Berdasarkan Gambar 9, perangkat ujian CBT telah berhasil terenkripsi menggunakan Algoritma RSA, sehingga keamaan data lebih terjaga. Berdasarkan hasil uji keamanan, chiperteks tidak bisa didekripsi dengan kunci yang tidak sesuai dengan ketentuan yang ada.

KESIMPULAN

Setelah dilakukanya pengembangan terhadap aplikasi *Computer Based Test* dengan Protokol *Two Central Facilities* yang menerapkan sistem *Central Legitimization Agency* (CLA) dan *Central Tabulating Facilities* (CTF) telah berhasil menciptakan sistem CBT yang terjaga keamanan datanya. Ditambah lagi adanya enkripsi pada data dengan Algoritma RSA yang dapat membuat keamanan data lebih terjaga. Dengan adanya penerapan Algoritma RSA, data yang tersimpan pada sistem berupa chiperteks. Chiperteks hanya bisa didekripsi menggunakan kunci yang telah ditentukan oleh sistem, sehingga selain kunci yang ditentukan data tidak bisa terbaca oleh siapapun.

DAFTAR PUSTAKA

Bishop, M. (2003). Computer Security Art and Science. *Pearson Education, Inc. Boston*.

Firdaus, C., Wahyudin, & Nugroho, E. P. (2017). Monitoring System with Two Central Facilities Protocol. *Jurnal UPI*, 1.

Kemendikbud. (2019, November 19). *Tentang UNBK*. Retrieved from Kemendikbud UNBK: https://ubk.kemdikbud.go.id/

Muharram, A. T., & Satrya, F. (2015). Rancang Bangun Sistem E-Voting Menggunakan Protokol Two Central Facilities. *Jurnal Informatik*, 37.

Nisha, S., & Farik, M. (2017). RSA Public Key Cryptography Algorithm – A Review. *IJSTR*, 187.

Poggio, J., Glassnapp, D., & Yang, X. (2005). A Com-parative Evaluation of Score Results from Com-puterized and Paper & Pencil Mathematics Test-ing in a Large Scale State Assessment Program. *The Journal of Technology, Learning, and As-sessment*, 4-30.

Saranya, Vinothini, & Vasumathi. (2014). A Study on RSA Algorithm for Cryptography. *IJCSIT*, 5708.

Schneir, B. (1996). Applied Cryptography. *Ed ke-2, Jon Wiley & Sons*.

Sireesha, J., & Chakchai, S.-I. (2005). *Secure Virtual Election Booth with Two Central Facilities.* Washington: Department of Computer Science Washington University.