USER MONITORING IN COMPUTER LABORATORY (Batam State Polytechnic)

Mira C. Kirana[1)], Tri Ramadani[2)], Afdhol Dzikri[3)], Nur C. Kushardianto[4)], Tresnawati D. Amdhani[5)], Enni Satria[6)]

[1, 2,3,4,5,6)] Batam Polytechnics
Informatics Study Program
Jl. Ahmad Yani, Batam Centre, Batam 29461, Indonesia
e-mail: mira@polibatam.ac.id[1)], ramadani@polibatam.ac.id[2)], afdhol@polibatam.com[3)], anung@polibatam.com[4)], dyah.amdhani@gmail.com[5)], ennisatria@gmail.com[6)]

ABSTRAK

Laboratorium komputer merupakan sarana yang sangat dibutuhkan pada lingkungan pendidikan.dan setiap aktivitas di dalam laboratorium komputer seharusnya bisa di monitor oleh penanggung jawab laboratorium. Penggunaan oleh mahasiswa bisa memberikan peluang terjadinya kerusakan terhadap fasilitas laboratorium, hal tersebut menyebabkan terhambatnya proses pembelajaran, sehingga dibutuhkan sebuah aplikasi yang bisa memberikan identitas dan aktivitas pengguna. Penelitian ini bertujuan untuk melakukan autentikasi identitas dan monitoring aktivitas pengguna berbasis client-server. Hasil analisa aktivitas praktikum di Laboratorium Komputer, terdapat dua kondisi yang terjadi, yaitu normal dan anomali supaya bisa mengidentifikasi kesesuaian penggunaan komputer di laboratorium.

Perancangan studi ini menggunakan use case yang terdiri dari dua aktor serta sepuluh interaksi yang disesuaikan dengan kebutuhan fungsional. Hal tersebut mendukung pengujian terhadap semua fungsi yang dibutuhkan, sehingga memberikan kesimpulan bahwa penelitian ini, baik dari sisi klien maupun server menunjukkan bahwa autentikasi dan pencatatan identitas, waktu akses serta aktivitas pengguna telah berhasil dilakukan.

***Kata Kunci**: monitoring, autentikasi, client, server*

ABSTRACT

The computer laboratory is educational tool which is needed in the educational environment and all activities in the lab should be monitored by the person in charge of it. Utilization of the facilities by students can lead of damage which cause inhibit in the learning process, therefore it is need an application that can provide a record of identity and user activity. This study aims to perform identity authentication and user activity monitoring based on client-server. The analysis of activities in the computer laboratory show that there are two conditions, normal and anomaly in order to identify the appropriateness of using a computer in a laboratory.

The design of this study has two actors with ten functional requirements. It supports testing of all the functions needed, thus concludes that the study, both from the client and server side indicates that the authentication, recording identity, access time and user activity has been successfully conducted.

***Keywords**: monitoring, authentication, client, server*

I. PENDAHULUAN

LABORATORIUM komputer merupakan sarana yang sangat dibutuhkan pada lingkungan pendidikan, dengan tujuan untuk menunjang proses pembelajaran. Setiap kegiatan yang dilakukan seharusnya mendapat pengawasan dari penanggung jawab laboratorium karena sangat penting untuk pendataan penggunaan laboratorium serta kapan saja laboratorium digunakan, laboratorium komputer juga membutuhkan suatu sistem informasi yang memudahkan proses kegiatan yang dilaksanakan, baik itu dalam pendidikan maupun perkantoran (Frizal Luthfi Hadyan dan Doro Edi, 2014). Hal tersebut untuk mencegah penyalahgunaan fasilitas laboratorium komputer sehingga pada akhirnya dapat menghambat proses pembelajaran.

Laboratorium komputer sudah menjadi kebutuhan di dunia pendidikan tinggi, yaitu universitas maupun politeknik. Hampir semua universitas sudah memiliki laboratorium komputer. Kebutuhan akan laboratorium komputer ini semakin meningkat. Tidak hanya jurusan yang berkaitan dengan pembelajaran komputer saja tetapi sekarang ini hampir semua jurusan sudah membutuhkan laboratorium komputer untuk menunjang pembelajaran lainnya. Sama halnya yang terjadi di Laboratorium Komputer Teknik Mesin Politeknik Negeri Batam, dimana kepala bidang laboratorium komputer sempat mengeluh bahwa

pernah terjadi kehilangan perangkat USB Wireless Mouse yang diduga diambil oleh mahasiswa yang menggunakan fasilitas di laboratorium komputer dan tidak mengetahui mahasiswa mana yang mengambilnya. Selain itu, mahasiswa diberi kebebasan untuk menggunakan aplikasi atau software yang terdapat di komputer, sehingga saat aplikasi atau software tersebut tidak bisa digunakan atau berada dalam keadaan rusak, maka instruktur praktikum atau kepala bidang laboratorium komputer juga tidak mengetahui siapa yang membuat kerusakan pada aplikasi atau software tersebut sehingga tidak bisa digunakan setelah jam perkuliahan berakhir atau berganti.

Biasanya *laboratorium* komputer ini terdiri dari beberapa komputer yang dihubungkan antara satu komputer dengan komputer lainnya dengan istilah *client-server*. Jaringan *client server* merupakan model jaringan yang menggunakan satu atau beberapa komputer sebagai *server* yang memberikan sumber dayanya kepada komputer lain (*client*) dalam jaringan. (Dony Ariyus dan Rum Andri, 2008). Bagian *server* ini digunakan sebagai penyedia layanan kepada komputer*client*. Karena meningkatnya akan penggunaan *laboratorium* komputer ini terkadang *server* tidak mampu mengelola serta memantau aktivitas semua *client*.

Selama ini, instruktur praktikum atau kepala bidang laboratorium komputer tidak mengetahui identitas mahasiswa yang telah menyalahgunakan fasilitas komputer dan kapan mahasiswa melakukan penyalahgunaan tersebut, dikarenakan sistem *login* mahasiswa untuk mengakses ke komputer *client* dibuat dengan menggunakan *username* yang sama dari masing-masing mahasiswa dan tidak menggunakan *password* komputer. Sehubungan aktivitas pada *laboratorium* komputer ini terkadang pengelola praktikum juga tidak mengetahui jika sebagian dari mahasiswa tidak melaksanakan kegiatan pembelajaran sebagaimana semestinya. Seperti bermain *game*, *browsing* hal yang tidak berkaitan dengan pembelajaran serta membuka aplikasi yang tidak berhubungan dengan materi pada saat pembelajaran berlangsung. Tidak adanya sistem pencatatan serta penyimpanan ke komputer *server* terhadap identitas mahasiswa yang menggunakan komputer *client* dan waktu akses mahasiswa serta laporan aktivitasnya, menjadi kelemahan dari keamanan komputer *client* di Laboratorium Komputer Politeknik Negeri Batam.

Berdasarkan permasalahan yang disampaikan, maka dibutuhkan sebuah aplikasi untuk melakukan autentikasi pengguna berbasis *client-server* serta monitoring aktivitas penggunaan computer. Autentikasi pengguna, dalam hal ini mahasiswa, menggunakan nim dan *password* serta kode program studi dari masing-masing mahasiswa yang telah didaftarkan oleh instruktur praktikum maupun kepala bidang laboratorium komputer di komputer *server* sebelum mahasiswa mengakses ke dalam komputer *client* di laboratorium komputer dan aplikasi autentikasi pengguna ini menerapkan sistem waktu pengaksesan komputer *client* bagi mahasiswa yang sudah diberi hak akses untuk dapat menggunakan komputer *client* setelah melalui proses *login.* Hak akses yang didapat oleh mahasiswa untuk menggunakan komputer *client* dilakukan dengan cara sistem menyesuaikan data mahasiswa yang terdaftar pada *database server* dengan hasil masukan mahasiswa setelah mengisi formulir *login* menggunakan nim dan *password* serta kode program studi di komputer *client* (Ventura, 2002). Selain untuk autentikasi juga harus bisa memantau aktivitas pengguna, aktivitas tersebut dikelompokkan menjadi dua bagian yaitu normal dan anomaly. Kondisi normal adalah jika mahasiswa membuka aplikasi yang dibutuhkan pada saat sesi praktikum, sedangkan anomali terjadi pada saat mahasiswa membuka aplikasi selain aplikasi yang diijinkan.

II. TUJUAN DAN KONTRIBUSI PENELITIAN

Tujuan penelitian yang hendak dicapai setelah mengalami pengembangan tujuan supaya bisa dimanfaatkan oleh semua jurusan, adalah:

1. Menghasilkan aplikasi yang dapat membantu instruktur praktikum atau kepala bidang laboratorium dalam mengidentifikasi mahasiswa yang menggunakan komputer client serta menampilkan aktivitas yang dilakukan mahasiswa pada waktu pembelajaran dari client ke komputer server.
2. Membuat laporan waktu pengaksesan pengguna komputer client di komputer server bagi yang telah berhasil mengakses (melalui proses login) ke komputer, berupa ID waktu akses, hari dan tanggal akses, nomor PC client, NIM dan Nama Mahasiswa yang mengakses komputer serta waktu login dan logout.
3. Memantau semua aktivitas pengguna computer Laboratorium berdasarkan kondisi normal dan anomaly.

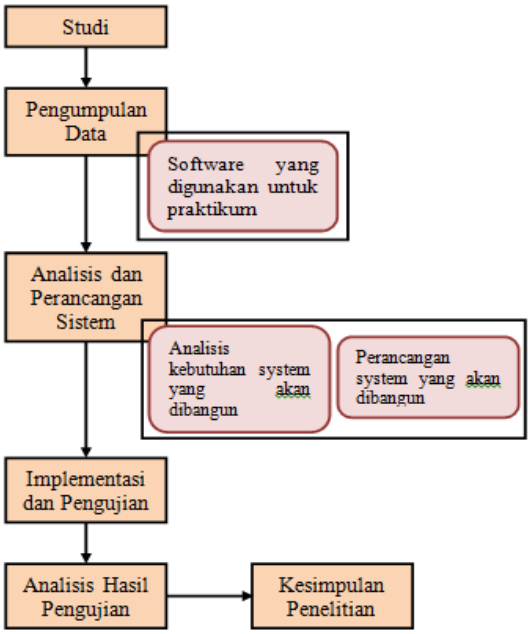
Beberapa kontribusi penelitian dapat dimanfaatkan oleh beberapa pihak yang terlibat dalam pelaksanaan magang seperti:

1. Membantu dosen praktikum dalam memantau aktivitas di computer mahasiswa selama proses praktikum berlangsung.
2. Membantu laboran dalam mengidentifikasi pengguna computer client di laboratorium.

Membantu mengetahui dan mencegah tindakan yang merugikan dalam proses praktikum di laboratorium komputer.

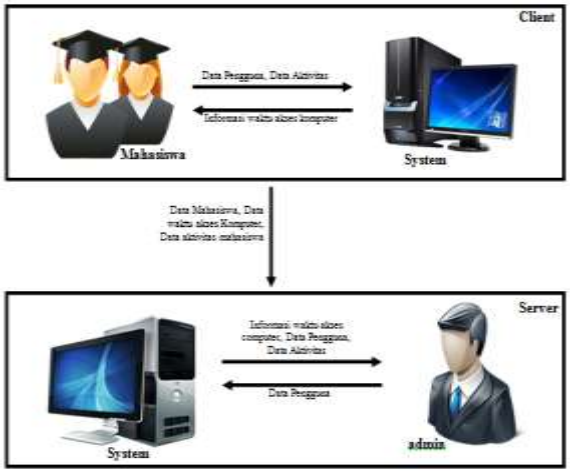
III. METODOLOGI

Perancangan system monitoring ini melalu 6(enam) tahap yang memiliki peran penting untuk setiap tahapnya, yaitu seperti di ilustrasikan pada gambar 1.



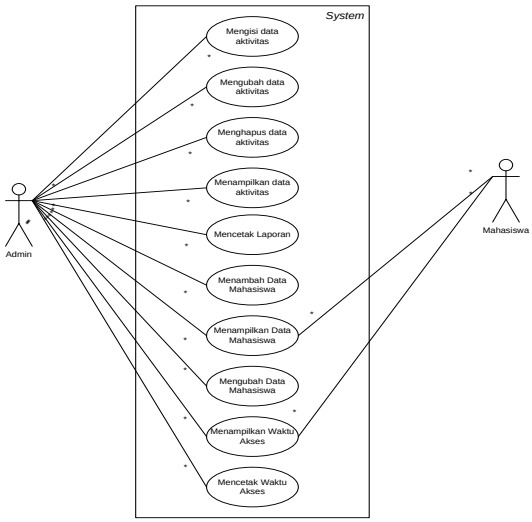
Gambar. 1. Metodologi Penelitian

Perancangan system dilaksanakan pada tahap ketiga, dimana studi ini menggunakan 2(dua) aktor yang berinteraksi dengan system, yaitu admin serta mahasiswa.



Gambar. 2. Deskripsi Sistem

Gambar 2 menjelaskan mengenai gambaran proses kerja system, dimana terdapat dua aplikasi yang masing-masing akan ditempatkan pada komputer *client* dan komputer *server* pengguna. Sebelum mahasiswa dapat mengakses di sisi *client*, terlebih dahulu admin mendaftarkan data mahasiswa melalui *server* kemudian mahasiswa dapat melakukan autentikasi melalui proses *login* dengan memasukkan data berupa NIM, *password* dan kode program studi. Sistem akan mencatat dan menyimpan data waktu akses *login* mahasiswa ke *database server* serta menampilkan informasi waktu akses *login* komputer ke sisi *client* untuk dilihat oleh mahasiswa, dimana dia juga bisa mengubah *password* dirinya sendiri. Semua data akan ditampilkan sebagai bentuk informasi dalam bentuk laporan. Selain itu admin bisa memasukkan aktivitas (nama aplikasi) untuk dijadikan rujukan bahwa hanya aplikasi yang terdaftar tersebut yang bisa dibuka oleh mahasiswa, serta mencatat semua aplikasi yang dibuka oleh mahasiswa untuk dijadikan laporan aktivitas seluruh mahasiswa oleh admin.



Gambar. 3. Use Case

Bedasarkan deskripsi sistem maka terdapat 10 (sepuluh) use case dengan 2(dua) actor yang menggambarkan kebutuhan fungsional untuk mencapai tujuan dari penelitian ini, hal ini ditunjukkan pada gambar 3.

IV. ANALISA HASIL

Terdapat dua fungsi utama dari aplikasi yang dibangun, yaitu untuk autentikasi identitas pengguna dan monitoring aktivitas pengguna. Proses autentikasi pengguna dilakukan di sisi klien dengan membuat start up windows yang mengharuskan pengguna untuk login, sehingga *Personal Computer* (PC) tidak bisa digunakan jika belum melakukan autentikasi.

Gambar 4 merupakan tampilan start up windows di sisi klien, dimana pengguna harus melakukan autentikasi jika akan menggunakan PC.

Gambar 4. Tampilan start up windows

Sedangkan gambar 5 merupakan catatan data autentikasi pengguna yang tersimpan oleh server, sehingga bisa digunakan untuk mencari pengguna terakhir dari PC klien tertentu jika dibutuhkan. Yang disimpan antara lain NIM, hari dan waktu akses hingga keluar.

Gambar 5. Tampilan data autentikasi pengguna pada server

Aplikasi yang telah didaftarkan adalah aplikasi yang boleh diakses sedangkan selain dari yang didaftar tidak dibolehkan. Jika saat client dijalankan dan telah login maka aplikasi selain yang ada pada daftar akan close otomatis. Misalkan pada gambar 6, dimana taskbar windows masih ada icon program yang masih berjalan, jika saat client dijalankan maka akan tertutup seperti gambar 7.


Gambar 6. Klien membuka aplikasi


Gambar 7. Aplikasi tertutup otomatis

Gambar 8 merupakan rincian aktivitas yang yg pernah dibuka oleh pengguna. Setiap aplikasi yang pernah dan sedang dibuka ditampilkan pada rincian aktivitas ini.

Gambar 8. Rincian aplikasi yang dibuka pengguna

V. KESIMPULAN

Berdasarkan hasil pengujian, kesimpulan yang bisa diambil adalah :

1. Aplikasi ini berhasil melakukan autentikasi pengguna, dimana tanpa melakukan autentikasi maka pengguna tidak bisa menggunakan PC sama sekali, karena start up windows hanya bisa dilakukan dengan proses autentikasi.
2. Server mampu mencatat dan menyimpan data pengguna yang telah melakukan autentikasi beserta data waktu kapan dia masuk dan keluar.
3. Aktivitas pengguna laboratorium bisa diketahui dari sisi server serta bisa menutup aplikasi yang dirasa tidak perlu digunakan, sehingga pengguna di sisi klien hanya bisa menggunakan aplikasi yang sesuai dengan yang telah masuk dalam daftar yang diperbolehkan.

DAFTAR PUSTAKA

[1] Frizal, L.H., Doro, E., 2014, Aplikasi *Laboratorium* Komputer Kontrol berbasis *ClientServer*, *Jurnal Sistem Informasi* 9(1), 63-71.
[2] Karhade, V., 2015, Computer Lab Monitoring System, International Journal on Recent and Innovation Trends in Computing and Communication 3(3), 1652 – 1656.
[3] Kelkar, B., Remote Lab Monitoring, 2016, International Research Journal of Engineering and Technology 3(3), 421 – 424.
[4] Setiawan, K., Wijaya, J., 2105, *Monitoring Beberapa Komputer di Laboratorium UPH Surabaya*.Jurnal Gema Aktualita 4(1):Surabaya: Universitas Pelita Harapan.
[5] Afdhal, 2010, *Perancangan* Sistem Keamanan Alternatif Jaringan Wireless LAN Dengan Metoda Autentikasi RADIUS, *Jurnal Komputasi Numerik dan Elektronika Terapan*, 7 (1), 1-8.
[6] Bhambure, J., dkk., *2014*, Secure Authentication Protocol in Client–Server Application using Visual Cryptography, *International Journal of Advanced Research in Computer Science and Software Engineering,*4(2), 556-560.
[7] Diartono, D.A., 2007, *Perancangan* Aplikasi Sistem Billing untuk Warnet Prabayar, *Jurnal Teknologi Informasi DINAMIK*, 12 (1), 75-87.
[8] Nayak, S.K., Mohapatra, S., dan Majhi, B., 2012, An Improved Mutual Authentication Framework for Cloud Computing, *International Journal of Computer Applications*, 52 (5), 36-41.
[9] Sari, R.F., dan Hidayat, S., 2006, Integrasi Mekanisme Autentikasi Aplikasi Web Server Dengan Metode LDAP : Studi Kasus Aplikasi SIPEG UI, *Jurnal Teknologi*, Edisi Khusus (1), 61-71.
[10] Sitorus, M., 2015, Aplikasi Keamanan Data Dengan Teknik Steganografi Menggunakan Metode End Of File (EOF), *Proceedings of the Informatics Conference*, Vol. 1, Jakarta, April 2016, A1-A7.
[11] Ventura, H., 2002, Diameter - *Next generation's AAA protocol,* Student Thesis, Linköping University, Department of Electrical Engineering, Swedia.