IMPLEMENTASI ALGORITMA ENKRIPSI CAESAR CIPHER DAN VIGENERE CIPHER PADA APLIKASI MOBILE DAN REST API DATA PERUSAHAAN PADA PT. CENTRAL CAPITAL FUTURES

Bagas Wahyu Utomo[1)], **Subandi**[2)]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : bagzinside@gmail.com[1)], subandionline@gmail.com[2)]

Abstrak

PT. Central Capital Futures merupakan salah satu perusahaan pialang berjangka yang berada di Indonesia. Sejauh ini PT. Central Capital Futures memiliki sebuah server data dimana berisi data perusahaan yang bersifat rahasia. Seluruh komunikasi data menggunakan REST API. REST API merupakan suatu metode komunikasi untuk perturakan data menggunakan protokol HTTP. Dalam prosesnya terjadi sebuah request data lalahdari suatu platform ke server data dan menghasilkan sebuah response berupa JSON yang nantinya akan diolah oleh platform tersebut untuk ditampilkan. Namun format response data yang ditampilkan pada mekanisme ini masih berupa JSON yang masih plaintext sehingga tidak akan menjamin kerahasiaan dan integritas datanya, jika terjadi serangan seperti penyadapan paket data. Penanggulangannya ialah dengan menerapkan algoritma kriptografi, yaitu kombinasi atas algoritma Caesar Cipher dan Vigenere Cipher pada saat proses pertukaran data, sehingga response yang tadinya berupa JSON yang masih plaintext akan berubah menjadi ciphertext yang masih harus di proses terlebih dahulu oleh platform agar dapat dibaca. Proses pengamanan ini dilakukan dengan membuat sebuah program yang nantinya akan mengintervensi setiap proses yang akan lewat. Diharapkan dengan adanya proses pengamanan ini dapat membantu menyelesaikan masalah keamanan komunikasi data pada PT. Central Capital Futures.

Kata kunci: REST API, Caesar Cipher, Vigenere Cipher

1. PENDAHULUAN

Teknologi informasi dan komunikasi semakin berkembang pesat seiring dengan munculnya sebuah permasalahan baru dalam bidang peyampaian informasi maupun komunikasi. Dunia teknologi informasi yang sudah terjadi saat ini terdiri atas media komunikasi sebagai suatu media penyampaian informasi dari suatu tempat ke tempat lainnya. Informasi yang ingin disampaikan berjalan atau tersalur melalui media komunikasi tersebut. Media komunikasi yang banyak digunakan tentu harus merupakan media yang paling sering maupun mudah dijangkau oleh semua orang. Contoh media komunikasi yang saat ini sering digunakan adalah *handphone*. Namun kemudahan penggunaan media komunikaasi oleh semua orang membawa dampak bagi keamanan bagi orang-orang yang menggunakan media tersebut. Informasi menjadi sangat mudah diambil, diketahui dan diubah oleh pihak yang tidak berkepentingan maupun tidak bertanggung jawab.

PT. Central Capital Futures merupakan salah satu perusahaan pialang berjangka yang berada di Indonesia, dimana pialang berjangka adalah suatu badan usaha yang melakukan kegiatan jual beli komoditi berdasarkan kontrak berjangka atas amanat nasabah dengan menarik sejumlah uang dan/atau surat berharga tertentu sebagai *margin* untuk menjamin suatu transaksi. Dalam persaingan perusahaan berjangka, PT. Central Capital Futures menciptakan sebuah produk sinyal *trading* berbayar tentunya hanya diperuntukkan untuk para nasabahnya. Dalam pendistribusian sinyal tersebut, digunakan sebuah aplikasi berbasis *mobile*. Tentunya dalam sebuah aplikasi *mobile* akan ada suatu komunikasi *request* maupun *response* data ke *server* data.

Aplikasi *mobile* sangat rentan apabila peretas melakukan *sniffing* melalui jaringan. Sehingga alamat *API* dapat diketahui oleh peretas maka bisa saja data dicuri bahkan dijual oleh pihak tersebut. Dengan demikian diperlukan pengamanan data *request* maupun *response* terhadap suatu *API*. Sehingga data yang beredar melalui jaringan akan aman terenkripsi. Algoritma kriptografi merupakan salah satu cara yang digunakan untuk menjamin keamanan data atau informasi. Algoritma yang biasa digunakan adalah *Caesar Cipher* dan *Vigenere Cipher*. Kedua algoritma tersebut mempunyai sebuah kunci simetris yang mengenkripsi plainteks secara digit per digit atau *byte* per *byte*.

2. LANDASAN TEORI

2.1. Keamanan Komputer

Keamanan dan kerahasiaan data merupakan sesuatu yang sangat penting dalam era informasi sekarang ini, dan telah menjadi kebutuhan karena arus informasi secara global telah menjadi tidak aman. Akan timbul banyak kerugian apabila informasi yang dikirim disadap atau dibajak oleh orang tidak berhak. Bahkan mungkin beberapa pengguna dari sistem itu sendiri mengubah data dan

informasi yang dimiliki menjadi sesuatu yang tidak kita inginkan (Prabowo 2015).

Keamanan data pada komputer tidak hanya bergantung pada teknologinya saja, tetapi juga dilihat dari aspek prosedur dan kebijakan keamanan yang diterapkan saat berjalan serta tingkat kedisiplinan sumber daya manusia. Jika *firewall* dan perangkat keamanan lainnya bisa disadap oleh orang yang tidak berhak, maka peran utama kriptografi untuk mengamankan data dan informasi dengan menggunakan teknik enkripsi sehingga data atau informasi tidak bisa dibaca (Prabowo 2015).

2.2. Komunikasi Data

Internet adalah salah satu terapan dari teknologi telekomunikasi yang banyak menggunakan protokol jaringan berbasis *Transmission Control Protocol/Internet Protocol* (TCP/IP), yaitu *Hypertext Transfer Protocol* (HTTP). HTTP adalah suatu protokol jaringan pada lapisan aplikasi pada TCP/IP yang digunakan untuk melakukan komunikasi data di web *world wide web* (WWW). Web memiliki fungsi sebagai media penyimpan data dan/atau media publikasi yang dapat diakses dari berbagai perangkat (Prabowo 2015).

2.3. Caesar Cipher

Caesar Cipher atau sering disebut juga subtitusi cipher merupakan penggantian setiap karakter dari *plaintext* dengan karakter lainnya. Teknik seperti ini disebut juga sebagai cipher abjad tunggal (Husein, 2014). Pada zaman Romawi kuno dikisahkan tentang Julius Caesar yang ingin mengirimkan satu pesan rahasia kepada seorang jenderal di medan perang. Pesan tersebut harus dikirimkan melalui seorang kurir, akan tetapi karena pesan tersebut mengandung rahasia, Julius Caesar tidak ingin informasi pada pesan tersebut sampai bocor di tengah jalan. Julius Caesar kemudian memikirkan cara mengatasinya, yaitu dengan melakukan pengacangan pesan menjadi suatu pesan yang tidak bisa dipahami oleh siapapun kecuali hanya dapat dipahami oleh jenderal saja. Tentu sang jenderal telah diberitahu sebelumnya bagaimana cara membaca pesan yang teracak tersebut karena telah mengetahui kuncinya (Rakhman et al. 2015).

Algoritma untuk *Caesar Cipher* adalah jika (a=2, b=3, dan seterusnya). *Plaintext* diberi simbol "PT" dan *ciphertext* adalah "CT", dan kunci adalah "KEY":

CT = E(PT) = (PT + KEY) mod (26)

Dari contoh di atas, enkripsi dapat dilakukan dengan rumus:

CT = E(PT) = (PT + 3) mod (26)

Rumus untuk melakukan dekripsi dari *ciphertext*:

CT = E(PT) = (PT - 3) mod (26)

2.4. Vigenere Cipher

Vigenere Cipher merupakan teknik kriptografi sederhana yang lebih aman. Dikembangkan dari metode *Caesar Cipher*, metode ini menggunakan karakter huruf sebagai kunci enkripsi. *Vigenere Cipher* juga merupakan *polyalphabetic substition cipher* (Salomon, 2003). Karakter huruf yang digunakan pada *Vigenere Cipher* yaitu A, B, C, ..., Z dan disamakan dengan angka 0, 1, 2, ..., 25. Proses enkripsi dilakukan dengan menulis kunci secara berulang. Penulisan kunci secara berulang dilakukan hingga setiap karakter pada pesan memiliki pasangan sebuah karakter dari kunci. Selanjutnya karakter pada pesan dienkripsi menggunakan metode *Caesar Cipher* dengan nilai kunci yang telah dipasangkan dengan angka (Arjana et al. 2012).

Plain Text	T	H	E	S	K	Y	I	S	F	A	L	L	I	N	G
Kunci	E	N	C	O	D	E	E	N	C	O	D	E	E	N	C
Cipher Text	X	U	G	G	N	C	M	F	H	O	O	P	M	A	I

Gambar 1. Contoh Enkripsi Menggunakan *Vigenere Cipher*(Prabowo 2015)

Contoh enkripsi pada Gambar 2.2, karakter pesan "Y" dienkripsi dengan kunci "E" dan menghasilkan *cipher text* "C". Hasil enkripsi didapatkan dari karakter pesan "Y" bernilai 24 dan karakter kunci "E" yang bernilai 4. Masing-masing nilai karakter ditambahkan 24+4=28. Karena 28 lebih besar dari pada 26 yang merupakan jumlah karakter yang digunakan, maka 28 dibagi dengan 26. Sisa pembagian tersebut adalah 2 yang merupakan nilai karakter "C". Proses enkripsi dapat dihitung dengan persamaan berikut (Arjana et al. 2012):

$$Ei = (Pi + Ki)\ mod 26$$

dimana Ei, Pi dan Ki merupakan karakter hasil enkripsi, karakter pesan dan karakter kunci. Sedangkan proses dekripsi dapat menggunakan persamaan berikut:

$$Di = (Ci - Ki)\ mod 26$$

dengan Di adalah karakter hasil dekripsi, Ci adalah karakter *cipher text* atau sandi, Ki adalah karakter kunci.

1) Contoh Permasalahan *Vigenere Cipher*

Kasus :

Plaintext : IGNATIUS
Key : MADE

Jawaban

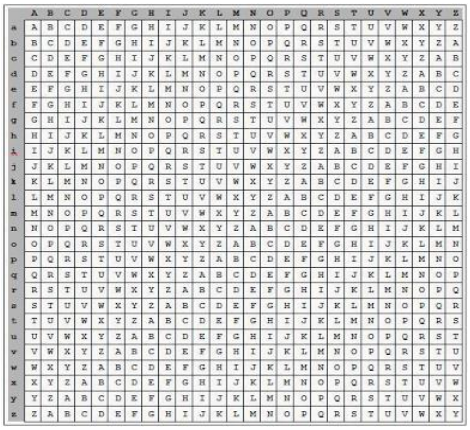
Berdasarkan tabel subtitusi

PlainText	8	6	13	0	19	8	20	18
Kunci	12	0	3	4	12	0	3	4
Hasil	20	6	16	4	31	8	23	22
CipherText/Output	U	G	Q	E	F	I	X	W

Gambar 2. Tabel Subtitusi (Husein 2014)

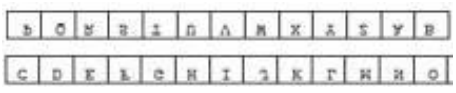
Hasil di atas berdasarkan perhitungan tabel subtitusi. Apabila terdapat angka misalnya 31 pada contoh di baris hasil maka dihitung 31 – 26 = 5 yaitu F (minus 26 karena banyaknya alphabet 26 huruf). Serta kunci yang lebih sedikit banyak karakternya dibandingkan *plaintext* maka akan diulang seperti pada tabel.

Ada juga metode lain yang dapat dilakukan untuk melakukan enkripsi dengan menggunakan metode *vigènere cipher* yaitu menggunakan *tabula recta* (disebut juga bujur sangkar *vigènere*) (Prabowo 2015).



Gambar 3. Tabula Recta Algoritma Kriptografi *Vigenere Cipher* (Susana et al. 2015)

Pada kolom paling kiri dari bujursangkar menyatakan huruf-huruf kunci, sedangkan baris paling atas menyatakan huruf-huruf *plaintext*. Setiap baris di dalam bujursangkar menyatakan huruf-huruf *ciphertext* yang diperoleh menggunakan *Caesar Cipher*, yang mana jumlah pergeseran huruf *plaintext* ditentukan nilai numerik huruf kunci tersebut misalkan (yaitu, a=2, b=3, c=4, …, z=26). Sebagai contoh, huruf kunci c (=8) menyatakan huruf-huruf *plaintext* digeser sejauh 4 huruf ke kanan (dari susunan alfabetnya), sehingga huruf-huruf *ciphertext* pada baris c adalah (Prabowo 2015):



Gambar 2. Potongan Tabula Recta Baris ke-C (Prabowo 2015)

Bujur sangkar *vigenere* digunakan untuk memperoleh *chipertext* dengan menggunakan kunci yang sudah ditentukan sebelumnya. Jika panjang kunci lebih pendek daripada

Plaintext : IGNATIUS
Key : MADEMADE

Untuk mendapatkan *ciphertext* dari teks dan kunci di atas, untuk huruf *plaintext* pertama I, ditarik garis vertikal dari huruf I dan ditarik garis mendatar dari huruf m, perpotongannya adalah pada kotak yang berisi huruf U. Dengan cara yang sama, ditarik garis vertikal dari huruf G dan lalu tarik garis mendatar pada huruf A, perpotongannya adalah pada kotak yang juga berisi bernisi huruf G. hasil enkripsi seluruhnya adalah sebagai berikut:

Plaintext : IGNATIUS
Key : mademade
Ciphertext/Output : UGQEFIXW

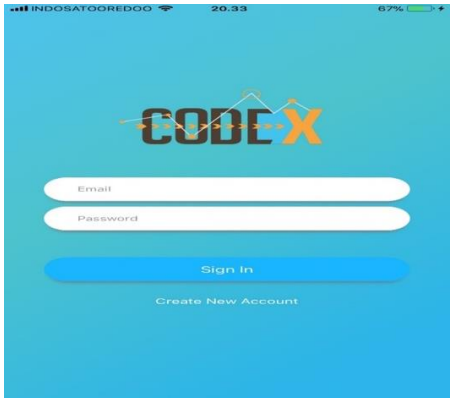
3. HASIL DAN PEMBAHASAN

3.1. Tampilan Layar

Berikut ini merupakan tampilan form yang terdapat pada aplikasi ini.

a. Tampilan Layar *Form Sign In*

Pada *form* pertama ini terdapat suatu tampilan *Sign In* terdapat dua inputan untuk dapat masuk ke halaman utama yaitu menggunakan *email* dan *password*. Disini juga terdapat *link* yaitu "*Create New Account*" yang akan membuka *form sign up*. Berikut ini adalah tampilan *form Sign In*.



Gambar 6. Tampilan Layar *Form Sign In*

b. Tampilan Uji Coba *Form Sign In*

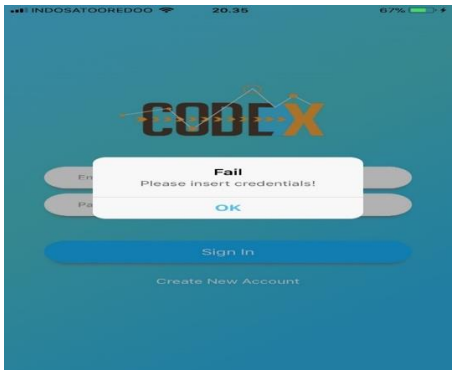
1) Tampilan Layar Uji Coba *Form Sign in*

Untuk dapat mengakses halaman utama user harus melakukan *Sign In* melalui *form Sign In* yang telah disediakan. Dengan *user* memasukkan *email* dan *password* yang digunakan untuk *Sign In*. Bisa dilihat pada gambar dibawah ini.

Gambar 7. Tampilan Layar Uji Coba *Form Sign in*

2) Tampilan Layar Pemberitahuan Tanda *Email* dan *Password* Salah

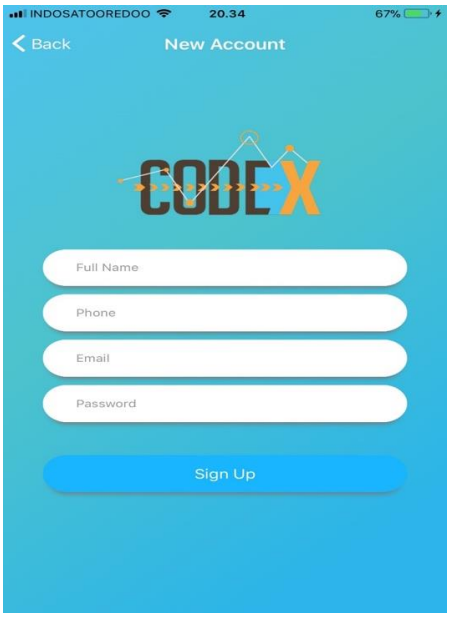
Lalu *user* diminta untuk memasukkan *email* dan *password* yang ada untuk bisa mengakses aplikasi atau masuk ke dalam halaman utama. Bisa dilihat pada gambar dibawah ini.



Gambar 8. Tampilan Layar Pemberitahuan Tanda *Email* dan *Password* Salah

c. Tampilan Layar *Form Sign Up*

Tampilan layar *form Sign Up* daoat digunakan oleh user untuk mendaftarkan *akun* mereka sehingga bisa masuk kedalam aplikasi. Dan nanti *user* dapat menggunakan fasilitas yang ada pada pada halaman utama. Berikut ini adalah tampilan layar *form Sign Up.*



Gambar 9. Tampilan Layar *Form Sign Up*

d. Uji Coba *Form Sign Up*

1) Tampilan Layar Uji Coba *Form Sign Up*

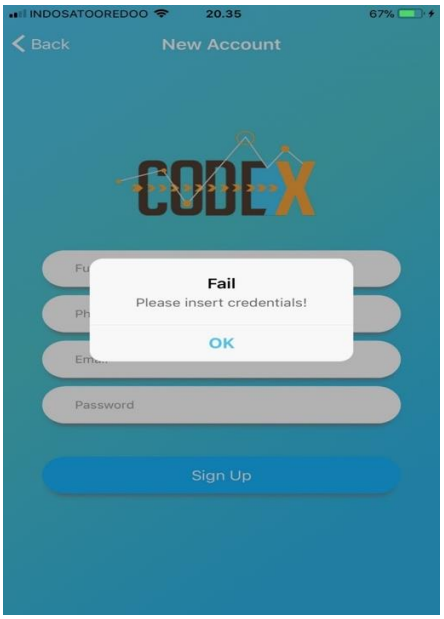
Pada tampilan *form Sign Up* ini, *user* dapat melihat beberapa field inputan data yang sudah diisi. Berikut ini adalah tampilan layar *form Sign Up.*

Gambar 10. Tampilan Layar Uji Coba *Form Sign Up*

2) Tampilan Layar Pemberitahuan Data Salah

Tampilan layar pemberitahuan jika sala satu data kosong. Sehingga akan muncul pemberitahuan dibawah nama bawah nama

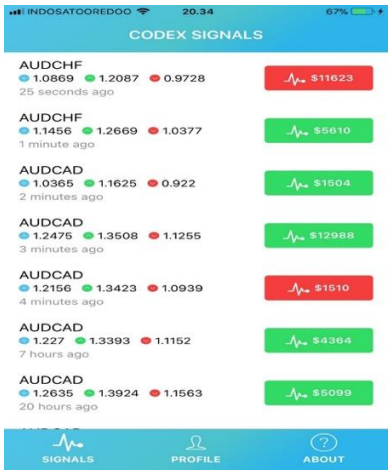
belum diisi. Berikut gambar pemberitahuan bisa dilihat dibawah ini.



Gambar 11. Tampilan Layar Pemberitahuan Data Salah

e. Tampilan Layar *Form Signal*

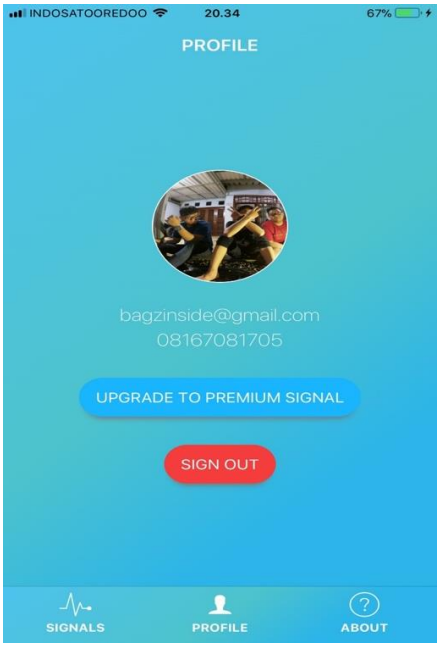
Tampilan layar *form signal* adalah tampilan yang memberitahukan kepada *user* untuk data trading yang ada dan sedang online. Disana ada beberapa info yaitu seperti waktu, *running trading* dan *take profit*. Pada *form signal* juga terdapat fungsi untuk membuka *form menu* lain seperti *form profile* dan *form about*. Bisa dilihat pada gambar dibawah ini:



Gambar 12. Tampilan Layar *Form Signal*

f. Tampilan Layar *Form Profile*

Tampilan layar *form profile* adalah tampilan yang memberitahukan atau memperlihatkan seputar info *profile* dari *user*. Untuk fungsi *upgrade to premium signal* ialah dimana untuk kualitas sinyal dalam *update signal* lebih baik atau mungkin lebih cepat dan juga hanya ada pada *form profile* untuk *user* melakukan perintah *sign out* dari aplikasi. Bisa dilihat pada gambar dibawah ini:



Gambar 13. Tampilan Layar *Form Profile*

g. Tampilan Layar *Form About*

Tampilan layar *form about* adalah tampilan yang memberi info seputar tempat dari *programmer* mulai melakukan riset. Dan juga disini terdapat informasi data dari *programmer* walau hanya sekilas. Disini ada fungsi untuk *user* membuka kembali *form menu* dari *form signal* dan *form profile*. Bisa dilihat pada gambar dibawah ini:

Gambar 14. Tampilan Layar *Form About*

3.2. Evaluasi Program

Evaluasi Program merupakan tahap terakhir yang perlu dilakukan dalam pengembangan suatu aplikasi. Evaluasi program bertujuan untuk mengetahui hasil yang telah dicapai dari aplikasi yang dibuat oleh pihak pengembang. Berikut adalah adalah evaluasi yang diperoleh:

a. Kelebihan Aplikasi

1) Aplikasi dirancang untuk dapat melakukan proses enkripsi dan dekripsi pada saat sedang melakukan pertukaran data.
2) Mempunyai menu *register* untuk mendaftarkan akun sehingga hanya *user* yang terdaftar yang dapat menggunakan.
3) Bisa di jalankan pada platform *Android* maupun *iOS*.

b. Kekurangan Aplikasi

1) Karena dibangun menggunakan *framework hybrid* yaitu *ionic*, maka tidak terasa seperti aplikasi *native* yang dibangun menggunakan bahasa pemrograman khusus device masing-masing pada umumnya.

Masih membutuhkan improvisasi dalam pengembangan aplikasi ini.

4. KESIMPULAN

Setelah melewati beberapa tahap penelitian serta pengujian pada program ini, dapat disimpulkan bahwa :

a. Ukuran data yang telah di enkripsi dan di dekripsi berubah, dikarenakan adanya perubahan data awalnya *plaintext* menjadi *ciphertext* yang ukurannya lebih panjang.
b. Yang dapat menggunakan aplikasi ini hanya user yang sudah terdaftar di dalam database perusahaan.
c. Mengurangi kemungkinan penyadapan data dari pihak yang tidak bertanggung jawab.

5. DAFTAR PUSTAKA

[1] Arjana, P.H. et al., 2012. Implementasi enkripsi data dengan algoritma. , 2012(Sentika), pp.164–169..

[2] Husein, M., 2014. IMPLEMENTASI CAESAR CIPHER UNTUK PENYEMBUNYIAN PESAN TEKS RAHASIA PADA CITRA DENGAN MENGGUNAKAN METODE LEAST SIGNIFICANT BIT. , pp.116–122.

[3] Prabowo, H.E., 2015. ENKRIPSI TEKS MENGGUNAKAN METODE VIGENERE CIPHER DENGAN PEMBENTUKAN KUNCI TAHAP.

[4] Rakhman, A.A. et al., 2015. IMPLEMENTASI ALGORITMA KRIPTOGRAFI RIVEST SHAMIR ADLEMAN (RSA) DAN VIGENERE CIPHER PADA GAMBAR BITMAP 8 BIT. , 14(2), pp.122–134.

[5] Susana, R., Nugraha, A. & Nataliana, D., 2015. Perancangan dan Realisasi Web-Based Data Logging System menggunakan ATmega16 melalui Hypertext Transfer Protocol (HTTP). , 3(1), pp.1–15.