SinarFe7
Seminar Nasional Fortei Regional 7

ISSN (Print) : 2621-3540
ISSN (Online) : 2621-5551

Rancang Bangun Sistem Token Rekening Air dengan Metode Hybrid (*Caesar Chiper and Rail Fence Chiper Transposition)* sebagai *Security System* Identitas Pin Token

[1]Mochamad Fiqri, [2]Diana Rahmawati, [3]Haryanto
[1 2 3] Teknik Elektro, Universitas Trunojoyo Madura, Bangkalan
[1]mochamadfiqri17@gmail.com, [2]diana.rahmawati@trunojoyo.ac.id, [3]Haryanto@trunojoyo.ac.id

Abstrak— Perusahaan Daerah Air Minum (PDAM) adalah sebuah perusahaan yang dikelola Badan Usaha Milik daerah (BUMD) kabupaten atau kota yang bergerak dalam pendistribusian air bersih. Pada tahun 2015, sistem token diciptakan untuk pembayaran PDAM. sistem token didapat dari hasil enkripsi dengan metode *caesar chiper*. Hasil enkripsi meliputi ID pelanggan dan nilai pulsa. Nomor token diperiksa oleh arduino pada eepromnya agar tidak terjadi inputan dua kali atau nomor token salah. Jika token belum diinputkan pada arduino, arduino akan membuka *solenoid valve*. Jika volume air penuh, solenoid valve akan menutup. Namun sistem tersebut menggunakan satu metode kriptografi sehingga mudah dideskripsikan. Dan memori eeprom arduino terbatas. Dalam penelitian ini dibuat sistem token rekening air dengan metode hybrid yaitu metode *caesar chipper* dan *transposition chipper rail fence.* Sistem tersebut terdapat basis data untuk menyimpan nomor token. Komunikasi data antara mikrokontroler dan basis data yaitu *Internet of Things*. Terdapat solenoid valve sebagai buka dan tutup aliran air. Dan water flow sensor berfungsi sensor debit dan volume. Pengujian keseluruhan sistem menghasilkan tingkat akurasi 90 %

Kata Kunci—Caesar chiper, Transposition chiper rail fence, solenoid valve, Internet of Things, water flow sensor.

Abstract - Municipal Waterworks (PDAM) is a company which is run by state-owned corporation (BUMD) of regencies or cities that are engaged in the distribution of clean water. In 2015, token system was created for PDAM payment method. Token system was obtained from encryption results by caesar chiper method. Encryption results cover customer ID and pulse value. The token numbers were checked by the arduino on its eeprom to avoid double inputs or incorrect token number. If token had not been entered in the arduino, the arduino would have opened the solenoid valve. If the water volume is full, the solenoid valve would be close. But the system uses one method of cryptographic, so it is easily described. And the eeprom memory of arduino is limited. In this research, the researcher used the token system of water with hybrid method, which is *Caesar chipper* and *transposition chipper rail fence.* The system has databases to save the token numbers. Communication of Data and microcontroller and database is called *Internet of Things*. There was solenoid valve as cover where the water flow is opened and closed. And water flow has functions as sensor of the flow and volume. The result of the entire testing yields accuracy of 90%

Keywords — Caesar chiper, Transposition chiper rail fence, mikrokontroler, solenoid valve, Internet of Things, water flow sensor

I. PENDAHULUAN

Perusahaan Daerah Air Minum (PDAM) adalah sebuah perusahaan yang dikelola Badan Usaha Milik daerah (BUMD) kabupaten atau kota yang bergerak dalam pendistribusian air bersih. Pada tahun 2015 diciptakan sistem pembayaran PDAM yang efisien. Yaitu dengan sebuah server yang membuat deretan angka menggunakan satu metode penyandian yaitu *caesar chiper*. Deretan angka tersebut meliputi nilai pulsa air dan ID pelanggan sehingga pada arduino melakukan pengecekan terhadap ID user dan nilai pulsa untuk membuka *solenoid valve*. Dan akan menutup otomatis ketika pulsanya habis. Pada arduino juga dilengkapi dengan fungsi *eeprom* yang berfungsi sebagai menyimpan nomor token agar tidak terjadi inputan dua kali[1].

Namun sistem tersebut hanya menggunakan satu metode kriptografi sehingga proses penyandiannya mudah dideskripsikan. Dan terbatasnya memori eeprom pada arduino uno. Dengan memanfaatkan teknologi dibuatlah sistem token rekening air dengan dua metode yaitu transposisi *chipper rail fence* dan *caesar chipper*. Nomor token didapat dari admin dengan aplikasi penjualan nomor token. Nomor token yang diperoleh akan diinputkan oleh *user* ke *mikrokontroler ATmega16*

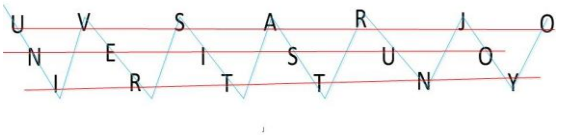
ISSN (Print) : 2621-3540
ISSN (Online) : 2621-5551

dengan *keypad* dan dikirim pada *web server*. Aplikasi pada admin mengambil data dari *web server* untuk diolah dan dikirim kembali hasil pengolahan pada *web server*. Kemudian *mikrokontroler* mengambil data hasil pengolahan. Jika hasil tersebut sesuai maka mikrokontroler menampilkan nilai volume dan solenoid valve membuka. *Solenoid valve* menutup jika jumlah volume air bernilai nol. Pada proses pengiriman dan pengambilan data dari *hardware* maupun *software* menggunakan komunikasi *Internet of things*.

A. Metode Transposition chiper rail fence

Transposition chiper rail fence adalah metode penyandian dengan melakukan acak posisi suatu huruf atau angka. Cara pengerjaan Huruf teks atau nomor ditulis denagn cara turun naik pada pagar imajiner. Pembacaan pada metode tersebut yaitu secara baris per baris[2].

Plaintext : UNIVERSITASTRUNOJOYO
Kunci : 3 baris



Gambar 1 huruf teks asli secara turun naik dalam sebuah pagar imajiner

Teks sandi menjadi UVSARJONEISUOIRTTNY.

B. Metode Caesar chiper

Dalam kriptografi, *caesar chiper* adalah metode penyandian penggeseran. Metode penyandian dengan cara mengilustrasikan dua set alfabet yaitu alphabet asli dan alphabet sandi. Alfabet sandi adalah alfabet yang disusun dengan cara menggeser alfabet ke kanan yang sesuai kunci berupa angka. Maka rumus untuk menjalankan metode *caesar chiper* sebagai berikut [3].

$$E(x)=((x - space + k) \bmod 13) + space \quad \text{.....(1)}$$

Pada rumus terdapat modulus 13 merupakan jumlah karakter yang dimulai dari nomor 48 sampai 60. nomor 48 sampai 60 didapat dari tabel ASCII.

Tabel 1. ASCII printable characters[3]

ASCII printable characters			
48 → 0	52 → 4	56 → 8	60 → <
49 → 1	53 → 5	57 → 9	
50 → 2	54 → 6	58 → :	
51 → 3	55 → 7	59 → ;	

Contoh penyandian sebuah pesan angka 17021 dengan kunci bernilai 3 sebagai berikut :

E"1"(49)=((49-32+3) mod 13)+32 = 52 →4
E"7"(55)=((55-32+3) mod 13)+32 = 58 → :
E"0"(48)=((48-32+3) mod 13)+32 = 51 →3
E"2"(50)=((50-32+3) mod 13)+32 =53→ 5

Jadi teks enkripsi menjadi 4:35

C. Internet of Things

Metode yang digunakan oleh *Internet of things* adalah nirkabel atau pengendalian secara otomatis tanpa mengenal jarak. Metode pada *Internet of things* merupakan jaringan nirkabel yang terhubung koneksi internet. Jadi, pengendaliannya tanpa mengenal jarak.

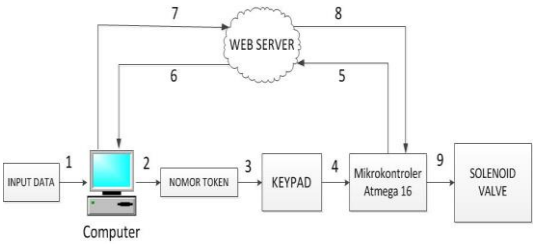
Cara kerja konsep Iot hanya menggunakan 3 elemen utama yaitu modul Iot berupa barang fisik, koneksi internet seperti modem dan router wireless, dan Cloud Data Center yang berguna sebagai penyimpanan aplikasi beserta database[5].

D. Tekanan Hidrostatis

Tekanan Hidrostatik merupakan tekanan yang disebabkan adanya gaya dari zat cair terhadap tempat yang mempunyai luas bidang dan kedalaman tertentu.

$$P = \rho.g.h \quad \text{.....(2)}$$

II. Metode Penelitian

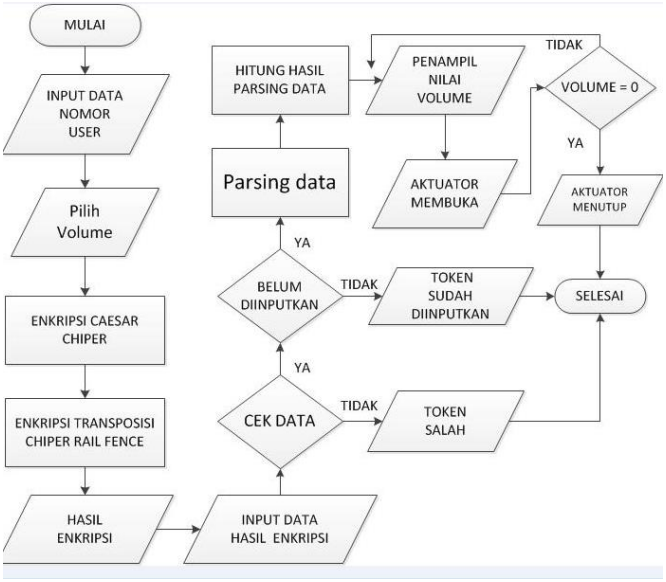


Gambar 2 Blok Diagram Sistem

Pada gambar 2 menjelaskan proses seluruh sistem. Nomor token didapat dari proses input data pada PC #. Nomor token akan diinputkan pada ATmega 16 melalui *keypad*. Nomor token pada ATmega 16 dikirim pada *web server* dan PC mengambil data terakhir pengiriman dari *web server*. Data tersebut diolah oleh PC dan

ISSN (Print) : 2621-3540
ISSN (Online) : 2621-5551

hasilnya dikirim kembali ke *web server*. Selanjutnya mikrokontroler mengambil data terakhir untuk membuka *solenoid valve* jika data tersebut sesuai.

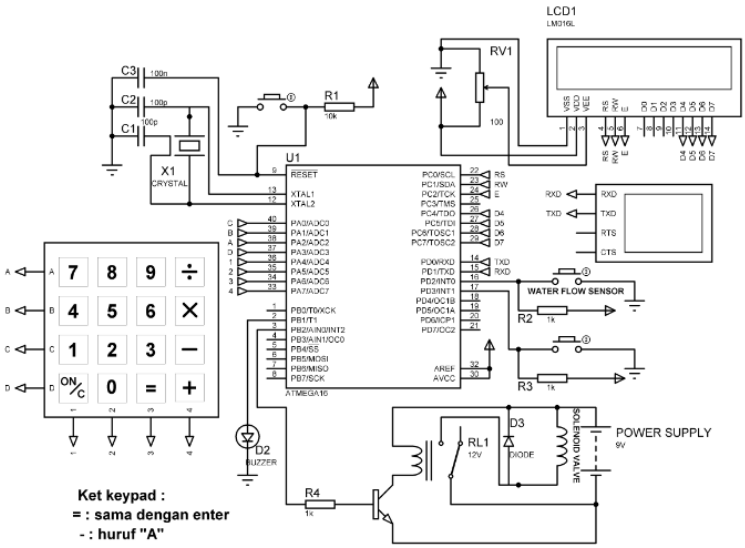


Gambar 3 Flowchart kerja Sistem

Proses enkripsi didapat dari gabungan ID user, pilih volume dan kode transaksi. Proses enkripsi pertama dengan metode *caesar chiper* dan dilanjutkan *transposition chiper rail fence*. Hasil enkripsi mengalami proses dua kondisi yaitu cek data dan belum diinputkan. Kondisi pertama adalah cek data. Jika hasil salah maka muncul pemberitahuan nomor token salah. Jika sebaliknya maka melanjutkan proses kondisi kedua yaitu belum diinputkan. Jika hasil salah muncul pemberitahuan token sudah diinputkan. Jika hasil sebaliknya maka data enkripsi mengalami proses parsing data. Hasil parsing data akan dihitung lalu ditampilkan hasilnya berupa volume sekaligus aktuator membuka hingga nilai volume yaitu nol.

A. Perancangan Perangkat keras

Pada perancangan perangkat keras memiliki beberapa perangkat *hardware*. Kontrol utama dari sistem tersebut menggunakan ATmega 16 yang terhubung dengan beberapa perangkat input atau output. Perangkat input meliputi *waterflow sensor*, *button* dan *keypad*. Sedangkan pada output terdapat *relay*, *solenoid valve*, *LCD 16x2* dan *buzzer*. Agar bisa berkomunikasi dengan PC, sistem tersebut terdapat *ESP 8266* yang merupakan komunikasi berbasis *Internet of things* .



Gambar 4 Perancangan Perangkat Keras

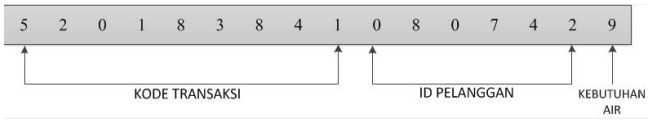
B. Perancangan Perangkat Lunak

Pada pembuatan aplikasi transaksi token rekening air dan komunikasi *Internet of things* menggunakan *Visual studio C#*. Sedangkan pada *web server* menggunakan web *thingspeak.com* dengan dua *fields*. *Fields* 1 berfungsi sebagai menampilkan nomor token dalam bentuk grafik. Sedangkan *fields* 2 menampilkan nilai dari aplikasi komunikasi *Internet of things.*

III. Hasil dan Pembahasan

A. Perancangan NomorToken

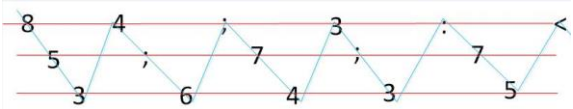
Kode deskripsi = 5201838410807429, k = 3



Gambar 5 Perancangan nomor token

Metode *Caesar chipper* :
Kode Enkripsi = 8534;6;743;3:75<

Metode *Transposition rail fence chipper* :



Gambar 8 Proses Metode Transposition Chiper

ISSN (Print) : 2621-3540
ISSN (Online) : 2621-5551

Nomor token= 84;3: < 5;7; 736 435

B. Pengujian Water Flow Sensor

Pengujian sensor dilakukan untuk mengetahui keakuratan sensor dengan output air 1 liter dengan jenis ember yang mempunyai tekanan yang berbeda dengan percepatan gravitasi 10 m/s^2.

Tabel 2. nilai tekanan dengan nilai kedalaman yang berbeda-beda

Jenis ember	h (tinggi air) cm	Tekanan (P) N/m^2
Ember A	30 cm	3000
Ember B	26 cm	2600
Ember C	22 cm	2200
Ember D	18 cm	1800
Ember E	14 cm	1400
Ember F	10 cm	1000

Pada *datasheet* sensor menunjukkan 450 putaran sama dengan 1 liter.

450=1 liter
450.z=1 liter
z=0.0022

nilai z menjadi pembuktian hasil volume nyata ketika 450 putaran. Tabel 4.1 pengukuran nilai volume ketika z = 0.0022 dengan input volume pilihan.

Tabel 3. nilai volume per 1 liter ketika z = 0.0022 dengan input volume pilihan

Jenis Ember	**output(liter)**	**Error (%)**
Ember A	1.09	9
Ember B	1.08	8
Ember C	1.1	10
Ember D	1.12	12
Ember E	1.19	19
Ember F	1.2	20

Tabel 3 menunjukkan volume yang dihasilkan tidak sesuai. Maka harus dilakukan kalibrasi pada putarannya.

1.13 liter - 1 liter = 0.13 liter
Putaran = 0.13/0.0022
Putaran = 59,09 putaran --≫ 59 putaran
Putaran = 450 putaran - 59 putaran
Putaran = 391 putaran
z baru=(1 liter) / (391 putaran)
z baru=0.0025

Tabel 4. nilai volume ketika z = 0.0025 dengan input volume pilihan

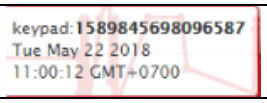
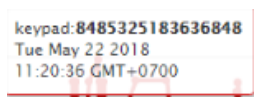
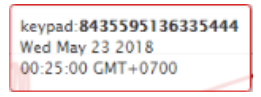
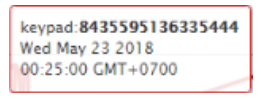
Jenis Ember	**output(liter)**	**Error (%)**
Ember A	1.00	0
Ember B	1.01	1
Ember C	1.00	0
Ember D	1.00	0
Ember E	1.00	0
Ember F	1.01	1
Rata-rata	**1.00**	**0.33**

Tingkat akurasi = 100 % - 0.33 %
= 99.63%

C. Pengujian Internet of things (IoT)

Pengujian IoT bertujuan untuk mengetahui respon *download* dan *upload* data dari *software* maupun *hardware* pada *web server*.

Tabel 5. Hasil pengujian respon *upload* data dari input *hardware* menuju server

No	Data Input	Data Server	Hasil
1			Sukses
2			Sukses
3			Gagal
4			Sukses
5			Gagal

Pengujian sebanyak 5 kali dengan sukses 3 kali dan 2 gagal. Maka tingkat akurasi sebagai berikut

$$= \frac{\text{pengujian + sukses}}{\text{pengujian + sukses + gagal}} \text{ x 100 \%}$$

$$= \frac{5 + 3}{5 + 3 + 2} \text{ x 100 \%}$$

= 80 %

Berdasarkan tabel 5 tingkat akurasi upload data *hardware* ke server sebesar 80 %. Nilai tersebut disebabkan karena kualitas jaringan internet provider kurang stabil sehingga server masih menampilkan data sebelumnya.

ISSN (Print) : 2621-3540
ISSN (Online) : 2621-5551

Tabel 6. Hasil pengujian respon *download* data dari server ke aplikasi

No	Data Server	Data Output	Hasil
1	keypad:1589845698096587 Tue May 22 2018 11:00:12 GMT+0700	1589845698096587	Sukses
2	keypad:8485325183636848 Tue May 22 2018 11:20:36 GMT+0700	8485325183636848	Sukses
3	keypad:8475365183636247 Tue May 22 2018 11:36:55 GMT+0700	8475365183636247	Sukses
4	keypad:8435595136335444 Wed May 23 2018 00:25:00 GMT+0700	8475365183636247	gagal
5	keypad:8435565156535443 Wed May 23 2018 00:37:18 GMT+0700	8435565156535443	Sukses

Pengujian sebanyak 5 kali dengan sukses 4 kali dan 1 gagal. Maka tingkat akurasi sebagai berikut

$$= \frac{5 + 4}{5 + 5 + 0} \quad \text{x } 100\ \%$$

$$= 90\ \%$$

Ketidaksesuaian data yang dihasilkan pada tabel 6 dikarenakan oleh ketidakstabilan internet yang menyebabkan tidak terkirimnya data. Sehingga pada output menampilkan data pengujian sebelumnya.

Tabel 7. Hasil pengujian respon *upload* data dari input aplikasi menuju server

No	Data Input	Data Server	Hasil
1	6	terima:6 Thu May 31 2018 00:37:27 GMT+0700	Sukses
2	3	terima:6 Thu May 31 2018 00:37:27 GMT+0700	Gagal
3	9	terima:9 Thu May 31 2018 00:49:47 GMT+0700	Sukses
4	5	terima:5 Wed May 23 2018 00:54:15 GMT+0700	Sukses
5	2	terima:2 Sun May 27 2018 15:21:15 GMT+0700	Sukses

Pengujian sebanyak 5 kali dengan 4 sukses dan 1 gagal. Maka tingkat akurasi sebagai berikut

$$= \frac{5 + 4}{5 + 4 + 1} \quad \text{x } 100\ \%$$

$$= 90\ \%$$

Pengujian pada tabel 7 menghasilkan tingkat akurasi 90 % dengan satu kali gagal. Ketidakberhasilan disebabkan karena kecepatan internet yang tidak stabil.

Tabel 8. Hasil pengujian respon *download* data dari server ke *hardware*

No	Data Server	Data Output	Hasil
1	terima:6 Thu May 31 2018 00:37:27 GMT+0700	1:6	Sukses
2	terima:3 Thu May 31 2018 00:19:59 GMT+0700	k=	Gagal
3	terima:9 Thu May 31 2018 00:49:47 GMT+0700	:9=	Sukses
4	terima:2 Sun May 27 2018 15:21:15 GMT+0700	:2=	Sukses
5	terima:5 Wed May 23 2018 00:54:15 GMT+0700	OK	Gagal

Pengujian sebanyak 5 kali dengan sukses 4 kali dan gagal. 2 kali. Maka tingkat akurasi sebagai berikut

$$= \frac{5 + 3}{5 + 3 + 1} \quad \text{x } 100\ \%$$

$$= 80\ \%$$

Ketidakberhasilan pada tabel 8 sebanyak dua kali. Hal tersebut disebabkan oleh ketidakstabilan internet. Sehingga dalam proses parsing data tidak tepat

D. Pengujian Keseluruhan Sistem

Pengujian sistem dilakukan mulai dari input token sampai kondisi solenoid. Pengujian pada nomor token mengalalmi proses perubahan ketika dikirim ke C# iot. Karena pada server tidak dapat menerima symbol – simbol. Maka perubahan tersebut adalah pada symbol ":" menjadi 0, ";" menjadi 1 dan "2" menjadi 0.

ISSN (Print) : 2621-3540
ISSN (Online) : 2621-5551

Tabel 9. Hasil. pengujian keseluruhan sistem

Perc.	Nomor token	*Hardware*	C# IoT	Kondisi solenoid	Hasil
1	8483 <65; 5:53 3434	8483 <65; 5:53 3434	8483 2651 5053 3434	membuka	Sukses
2	84<3< 9 5;8 <834 434	84<3< 9 5;8 <834 434	84232 9 518 2834 434	Membuka	Sukses
3	84;3< 6 5;3 <636 33;	87;3< 6 5;3 <936 30;	87132 6 513 2936 30;	Menutup	Sukses
4	8483 <65; 5:53 3434	8483 <65; 5:53 3434	8483 2651 5053 3434	menutup	Sukses
5	84633 6 5;3 <335 848	84633 6 5;3 <335 848	8483 2651 5053 3434	menutup	Gagal

Pengujian dilakukan menghasilkan tingkat akurasi sebagai berikut

$$= \frac{5 + 4}{5 + 4 + 1} \quad \text{x } 100\ \%$$

$$= 90\ \%$$

Tingkat keberhasilan pada pengujian tabel 9 sebanyak 4 kali. Parameter keberhasilan pengujian dapat dilihat dari nomor token pada *hardware* dan *C#* yang sama. Ketidaksamaan antara *hardware* dan *C#* disebabkan jaringan internet yang tidak stabil.

IV. Kesimpulan

Berdasarkan hasil pengujian rancangan dan pembahasan yang telah diuraikan, maka dapat diperoleh kesimpulan :

1. Pada penggunaan metode caesar chiper dan transposition chiper rail fence mempunyai sifat penyandian yang lemah jika penerapannya secara individu. Namun jika penggabungan dua metode tersebut dilakukan maka sifat penyandiannya cukup kuat.
2. Pada pengujian *water flow sensor* tingkat akurasi yang didapat adalah 99.67 %. Data tersebut diperoleh dari hasil pengujian yang mehasilkan error 0.33 % dengan membandingkan dengan gelas ukur atau timbangan digital.
3. Pada keseluruhan pengujian *Internet of Things* dismpulkan pengaruh kualitas jaringan yang mempengaruhi tingkat keberhasilan *download* data ataupun *upload* data.
4. Pada pengujian keseluruhan sistem, sistem dapat berjalan dengan baik jika nomor token pada *hardware* sama. Meskipun solenoid valve menutup. Pengaruh Kualitas internet mempengaruhi tingakt keberhasilan pengujian

Daftar Pustaka

[1] Musyafa, M., Rasmana, S., & Susanto, P. (2015). *Rancang Bangun Sistem Prabayar Pada Pdam*. Journal of Control and Network Systems , Vol. 4, No. 1 (2015) 01-06 .

[2] Basuki, A., Pranita, u., & Hidayat, R. (2016). *Perancangan Aplikasi Kriptografi Berlapis Menggunakan Algoritma Caesar, Transposisi, Vignere, Dan Blok Chiper Mobile*. Seminar Nasional Teknologi dan Multimedia 2016. ISSN: 2302-3805.

[3] Latifah, R, Ambo, S, & Kurnia, S. (2017). *Modifikasi Algoritma Caesar chiper dan rail fence untuk peningkatan keamanan teks alfanumerik dan karakter khusus*. Seminar Nasional Sains dan Teknologi 2017. e-ISSN : 2460-8416.

[4] Heydari, M., & Senejani, M. N. (2014). *Automated Cryptanalysis of Transposition Ciphers Using Cuckoo Search Algorithm* . International Journal of Computer Science and Mobile Computing , Vol. 3, Issue. 1, January 2014, pg.140 – 149

[5] Sasmoko, Dani & Wicaksono, Yanuar A. (2017*). Implementasi Penerapan Internet Of Things (Iot) Pada Monitoring Infus Menggunakan Esp 8266 Dan Web Untuk Berbagi Data*. Jurnal Ilmiah Informatika Vol. 02, No. 01, Juni 2017.

[6] Suharjono, A., Rahayu, L., & Afwah R. (2015). *Aplikasi Sensor Flow Meter Untuk Mengukur Penggunaan Air Pelanggan Secara Digital Serta Pengiriman Secara Otomaris Pada Padam Kota Semarang*. Jurnal TELE Volume 13 Nomor 1 Edisi Maret 2015.