

SISTEM PERPARKIRAN PRABAYAR BERBASIS MIKROKONTROLER AT89C52

Abdul Jabbar Lubis, Evri Ekadiansyah

ABSTRAK

Sistem perparkiran konvensional yang ada saat ini seringkali rentan terhadap manipulasi dalam tarif retribusinya. Untuk memperkecil manipulasi tarif ini, dibuatlah mekanisme sistem yang terkontrol bagi para pengguna jasa perparkiran. Sistem ini dirancang sesederhana mungkin dengan tiga buah perangkat utama yaitu: Chip pada pengguna jasa perparkiran, perangkat keras sistem jasa perparkiran pada pengelola perparkiran dan komputer.

Keyword : Mikrokontroler AT89C52, Smart Card, Sistem Parkir

A. PENDAHULUAN

Sistem perparkiran di negara kita ini secara umum masih bersifat konvensional. Artinya setiap pengguna jasa perparkiran bila akan memarkirkan Kendaraanya harus melapor kepada seorang petugas penjaga perparkiran untuk menerima karcis retribusi perparkiran. Dan terkadang banyak para petugas perparkiran yang *ilegal*. Dalam artian melakukan pemungutan parker dimana saja tanpa mengindahkan peraturan yang ada. Sehingga disuatu sisi rentan dengan manipulasi dan tentunya akan merugikan pemerintah.

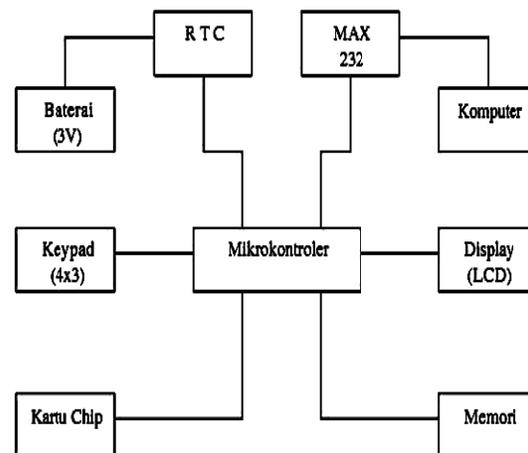
Oleh karena itu pada penulisan makalah kali ini penulis ingin mencoba memberikan sebuah gambaran dalam bentuk perancangan untuk mengatasi problem perparkiran yang ada di negara kita ini. Dalam perancangan dan perancangan system perparkiran ini sebenarnya hanya menggunakan perangkat yang sederhana yaitu :

1. Chip: Merupakan tempat untuk menyimpan identitas pengguna jasa perparkiran sekaligus tempat menyimpan saldo pembayaran perparkiran. Mengingat sistem yang digunakan adalah prabayar.
2. Chip Reader: pada pengelola jasa perparkiran yang berfungsi sebagai pembaca identitas yang dimiliki pengguna jasa perparkiran.
3. Komputer: Sebagai media tampilan sekaligus pemroses data.

B. METODE PERENCANAAN DAN PERANCANGAN

1. Perencanaan Perangkat keras

Perancangan perangkat keras meliputi : Penyediaan mikrokontroler single chip menggunakan AT89C52 sebagai pengendali system yang akan dibuat. Berikut blok diagram dari perancangan sistem perparkiran prabayar menggunakan mikrokontroler AT89C52.



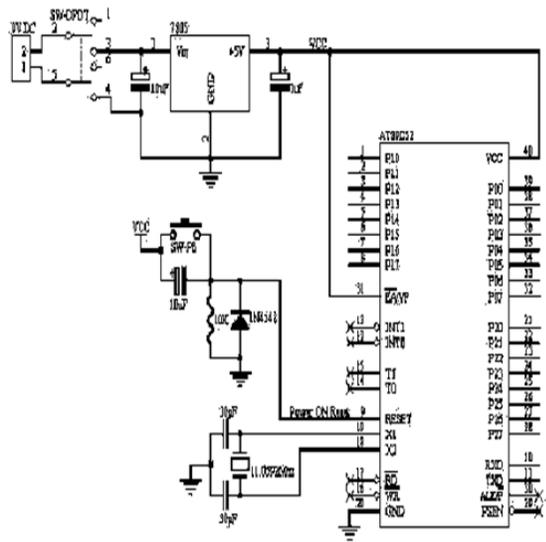
Gambar 1. Blok Diagram sistem perparkiran

2. Perencanaan komponen

Adapun komponen yang digunakan untuk mengimplementasikan perancangan blok diagram di atas kedalam wujud aslinya antara lain :

- a. Catu Daya
- b. Serial RTC (Real Time Clock) sebagai penghitung waktu yaitu tanggal, bulan dan tahun serta jam. Sedapat mungkin bias menggunakan IC DS 1302 sebab memiliki keunikan yaitu dapat menghitung hingga tahun 2100. Serial RTC ini berfungsi mencatat dan menghitung waktu keluar dan masuk dari pengguna jasa perparkiran.
- c. MAX 232 merupakan sebuah IC yang berfungsi sebagai driver dan receiver dengan computer
- d. Data – Data akumulasi saldo dapat dibangun menggunakan akses
- e. Battre untuk membackup tegangan Serial RTC
- f. Keypad
- g. Display LCD
- h. Chips standart ISO 7816

3. Perancangan Perangkat keras menggunakan mikrokontroler AT89C52.



Gambar 2. Rangkaian Sistem Kendali

Rangkaian diatas berfungsi mengontrol kerja perangkat yang dirancang. Dimana identitas pemilik yang telah tersimpan pada database akan dibaca oleh reader dan disesuaikan dengan data – data sebelumnya yang telah ada. Dikarenakan perancangan ini menggunakan sistem pembayaran sebelum digunakan (prabayar), maka sistem harus dirancang sedemikian rupa agar tidak terjadi kesalahan pada proses

penghitungan sisa saldo dalam chip yang terprogram.

Identitas sipemilik tersimpan dengan menggunakan sebuah chip yang mirip dengan smart card. Standar Internasional untuk protokol yang paling banyak digunakan dalam teknologi smart card ini adalah ISO 7816. Meskipun demikian, terdapat pula beberapa standar lain yang digunakan. Smart card menyimpan dan memproses informasi melalui rangkaian elektronik yang ada di dalam silikon yang dalam substrat plastik dari body-nya. Terdapat dua jenis smart card yang paling banyak digunakan yaitu intelligent smart card yang terdiri atas sebuah mikroprosesor dan mampu membaca, menulis, dan menghitung, seperti halnya sebuah mikrokomputer. Serta memory card, tidak memiliki mikroprsesor dan hanya digunakan untuk menyimpan informasi saja. memory card menggunakan security logic untuk mengatur akses dari memori. Meskipun demikian, sesungguhnya terdapat lima buah jenis smart card yang ada saat ini yaitu :

- a. Memory Card
- b. Processor Card
- c. Electronic Purse Card
- d. Security Card
- e. JavaCard

Secara umum ada 3 jenis memori [ISO7816-95] yang digunakan :

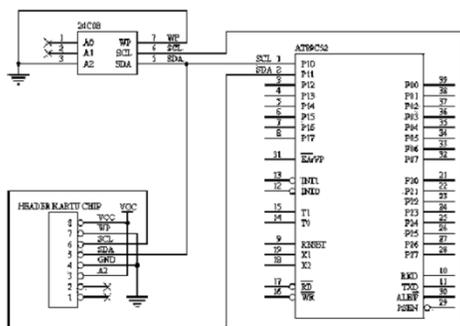
- a. **ROM (Read Only Memory)**, berfungsi untuk menyimpan program utama dan sifatnya permanen.
- b. **RAM (Random Access Memory)**, berfungsi untuk menyimpan data sementara ketika proses sedang berjalan atau hasil penghitungan selama mengeksekusi perintah. Data yang disimpan di dalamnya akan hilang begitu *smartcard* dicabut (*power* hilang).
- c. **EEPROM (Electrically Erasable Programmable Read Only Memory)**, berfungsi untuk menyimpan program dan data yang sewaktu-waktu bias diubah. Seperti halnya *hard disk* pada komputer, jenis memori ini akan tetap menyimpan data meskipun tidak ada *power*(permanen).

Ada 2 tipe *smartcard*, yaitu *smartcard* yang mempunyai mikroprosesor dan menawarkan kemampuan membaca, menulis dan melakukan

penghitungan, seperti mikrokomputer kecil. Yang kedua adalah *smartcard* memori yang tidak mempunyai mikroprosesor dan digunakan hanya untuk tempat menyimpan. *Smartcard* memori menggunakan *security logic* untuk mengatur akses ke memori. Secara komersial, industri membuat *smartcard* dalam beberapa varian, yaitu:

- a. **Memory cards.** *Smartcard* jenis ini hanya berfungsi untuk menyimpan data, tidak mempunyai *processor* atau sistem keamanan yang canggih melainkan hanya perlindungan fisik (karena *smartcard* bersifat *tamper proof*).
- b. **Memory protected cards.** *Smartcard* jenis ini mempunyai sistem keamanan yang lebih canggih daripada *memory cards*, misalnya mekanisme *password* untuk mengakses *smartcard*.
- c. **Microprocessor cards.** *Smartcard* jenis ini mempunyai *processor* sehingga dapat melakukan komputasi walaupun terbatas. Kemampuannya antara lain mengorganisasikan berkas (*file*) yang dilindungi dengan *password*.
- d. **Java cards.** *Smartcard* ini dilengkapi dengan Java Virtual Machine sedemikian hingga dapat dimasukkan berbagai program ke dalamnya.
- e. **Public key cards.** *Smartcard* ini mendukung *public key cryptography* (kriptografi asimetris) sehingga proses enkripsi/dekripsi dapat dilakukan secara internal dan dapat menyimpan *key*.

4. Rangkaian Reader, memory dan kartu chip.



Gambar 3. Rangkaian header, memory dan kartu chip

Rangkaian diatas berfungsi untuk menyelaraskan sistem kerja perangkat. Identitas pemilik yang sudah tersimpan dalam chips atau yang lebih dikenal dengan *smartcard* akan dibaca oleh reader. Lalu reader yang terhubung dengan mikrokontroler AT89C52 akan berkomunikasi dengan komputer dan akan menyesuaikan data pada chips dengan data yang terdapat dalam database pada komputer. Masing-masing perusahaan menyediakan protokol yang berbeda untuk berkomunikasi dengan *reader*. Komunikasi dengan *smartcard* berdasarkan format APDU (*Application Protocol Data Unit*). APDU merupakan unit dasar untuk pertukaran paket di dalam *smartcard*. Komunikasi antara kartu dengan *reader* dilakukan dengan APDU[ISO7816-95]. APDU dinyatakan sebagai data paket yang berisi perintah lengkap atau respon yang lengkap dari kartu. Untuk menyediakan fungsionalitas seperti ini, APDU mendefinisikan struktur yang didefinisikan dalam beberapa dokumen ISO 7816. ISO mendefinisikan standar bagaimana aplikasi berkomunikasi dengan *smartcard*. Sayangnya, ISO tidak mendefinisikan standar untuk berkomunikasi dengan *reader*. Sehingga untuk mengirim perintah ke kartu, pertama pemrogram perlu menemukan *command* yang dimengerti oleh kartu, kemudian membungkus *command* tersebut dengan ISO *command* paket, kemudian dibungkus lagi dengan pembungkus yang diperlukan oleh *reader*. Model *master-slave* digunakan di mana *smartcard* selalu memainkan posisi yang pasif. Dengan kata lain, *smartcard* selalu menunggu perintah APDU dari terminal. Kemudian *smartcard* mengeksekusi aksi yang ditentukan di dalam APDU dan mengembalikannya ke terminal dengan respon APDU. *Command* APDU dan respon APDU dipertukarkan antara kartu dan terminal. Gambar di bawah adalah format *command* dan respon APDU. Struktur APDU didefinisikan dalam ISO 7816-4.

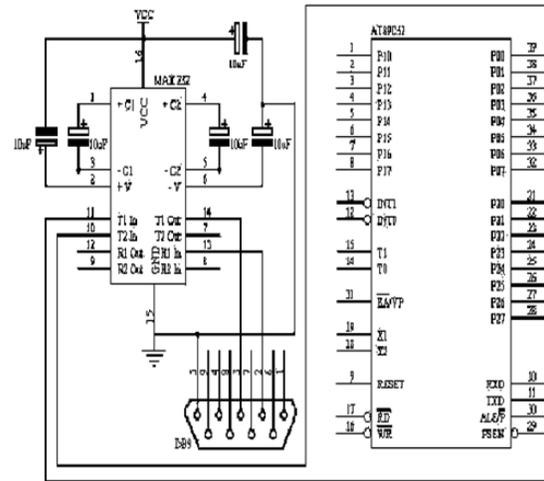
Header terdiri dari 4 field: *class* (CLA), perintah (INS) serta parameter 1 dan 2 (P1 dan P2). Masing-masing *field* berukuran 1 byte :

- a. CLA: *class* byte. Di beberapa *smartcard* digunakan untuk mengidentifikasi aplikasi.
- b. INS: *Instruction* byte. Byte ini menyatakan kode instruksi/perintah.

- c. P1 dan P2: Parameter byte. Menyediakan kualifikasi lebih lanjut untuk perintah APDU.
- d. *Conditional body* terdiri dari 3 *field*, yaitu Lc, datafield dan Le.
- e. Lc menyatakan jumlah byte di dalam *data field* dari *command* APDU, *Data field* menyatakan data yang diperlukan oleh *command* APDU.
- f. Le menyatakan jumlah maksimal dari byte yang diharapkan di dalam *data field* dari respon APDU.
- g. Respon APDU terdiri dari *conditional body* dan *mandatory trailer*.
- h. *Conditional body* berisi *data field* yang menyatakan data yang diperlukan oleh respon APDU.
- i. *Mandatory trailer* terdiri dari *status byte* SW1 dan SW2 menyatakan status proses dari *command* APDU di dalam kartu.

kekomputer yang berfungsi untuk menyimpan database sipengguna jasa parkir.

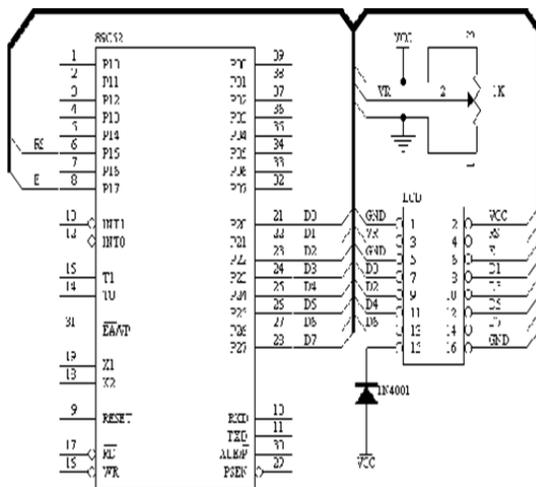
6. Rangkaian mikrokontroller AT89C52 dan MAX 232



Gambar 6. Rangkaian mikrokontroller AT89C52 dan MAX 232

Rangkaian ini terhubung ke port serial atau DB-9. Rangkaian inilah yang nantinya akan berkomunikasi dengan computer untuk membaca persesuaian data yang terdapat pada perangkat masukan yakni chip smartcard milik si pengguna dengan data yang terdapat pada database computer.

5. Rangkaian mikrokontroller AT89C52 dan Display LCD



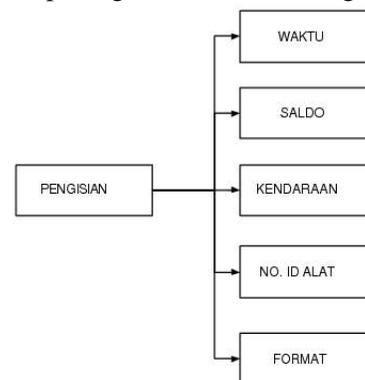
Gambar 5. Rangkaian mikrokontroller AT89C52 dan Display LCD

Pada rangkaian ini akan menghasilkan tampilan berupa identitas sipemilik, dan sisa saldo yang terdapat dalam smart card milik si pengguna jasa parkir. Rangkaian utama yakni mikrokontroller AT89C52 ini merupakan bridge untuk seluruh rangkaian yang ada. Sebab mikrokontroller ini terhubung langsung

7. Perencanaan Perangkat Lunak

Perancangan Perangkat Lunak dikelompokkan menjadi 2 bagian yaitu :

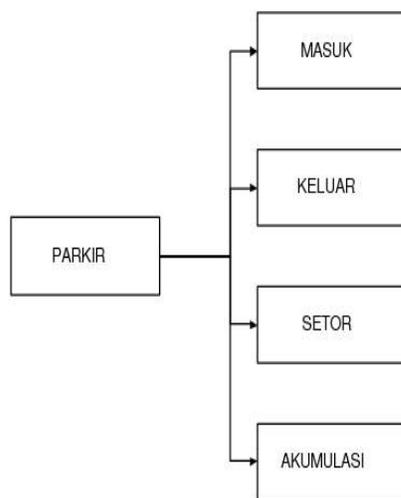
- a. Perangkat lunak untuk pengisian
- b. Dan perangkat lunak untuk bagian parkir.



Gambar 7. Rancangan Pengisian id

Pada perancangan bagian pengisian ini dilihat berdasarkan beberapa ketentuan yaitu :

- a. Waktu: Yaitu melihat waktu masuk dan waktu keluar si pengguna jasa perparkiran.
- b. Saldo: Yaitu tarif retribusi perparkiran yang telah diisikan kedalam chip dengan nilai nominal sesuai yang ditentukan oleh pihak penyelenggara parkir dan pengelola perparkiran.
- c. Kendaraan: Dilihat dari 2 jenis yaitu Kendaraan roda 2 dan Roda 4.
- d. Identitas Kendaraan: Dilihat berdasarkan No. Pelat Kendaraan bermotor.



Gambar 8. Rancangan bagian parkir

Selanjutnya pada bagian pengelola perparkiran dilihat dengan beberapa tahapan, yaitu: waktu masuk, waktu keluar dan penyetoran tarif retribusi perparkiran yang diambil langsung pada chips si pemilik Kendaraan. Dan setelah dikurangkan saldo yang terdapat pada chips maka akan diakumulasikan dengan saldo sebelumnya untuk kemudian dikurangkan. Sehingga yang tersisa saja yang dapat digunakan.

Smartcard kartu parkir ini mengeluarkan beberapa data jika mereka di *reset* atau dimasukkan ke alat pembaca. Ini disebut “*answer to reset*” atau ATR. ATR akan memberitahukan informasi mengenai pembuat *smartcard* (*issuer*) tersebut dan protokol yang seharusnya digunakan untuk berkomunikasi. Untuk menyandikan *byte* dapat menggunakan “*direct convention*” yaitu langsung

mengkomplemenkan *bit* atau “*inverse convention*” yaitu *bit* dibalik dan dibaca dari belakang. Protokol yang biasa digunakan disebut T=0 yaitu protokol paling sederhana dan T=1 yaitu protokol lebih kompleks dan memiliki lapisan jaringan tambahan. Contoh serangan yang dapat dilakukan a.l.:

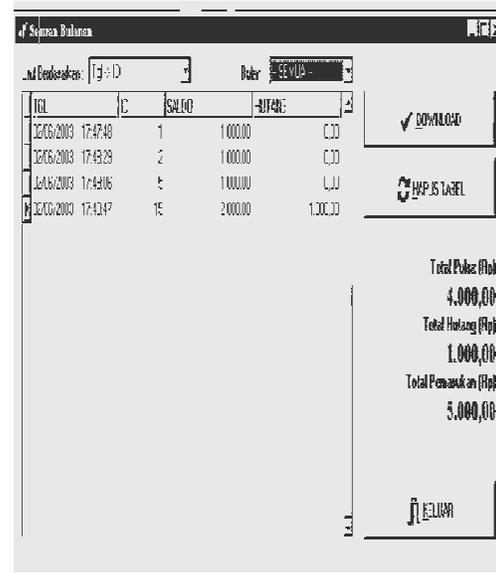
- a. Pengujian jenis *smartcard* : *smartcard* magnetik atau *smartcard* dengan *microkontroler*.
- b. Lihat dalam ATR : tentukan teknik penyandiannya dan protokol yang digunakan.
- c. Menebak instruksi yang digunakan, ada beberapa cara :
- d. Coba semua kemungkinan. *Dumb mouse* beroperasi pada 9600 *baud* sehingga walaupun banyak *smartcard*, *dumb mouse* dapat bekerja dua kali lebih cepat. Hal ini berbahaya, karena seseorang dapat mengeksekusi instruksi yang merusak, mengkosongkan atau mem-*block smartcard*.
- e. Melakukan *eavesdrop* pada komunikasi sesungguhnya dengan menggunakan alat *login*. Alat *login* dapat terlihat sebagai perpanjangan kawat antara *smartcard* dan terminal. Setiap *byte* yang dikirim dari atau ke *smartcard* dapat diawasi dan membantu untuk mengerti perintah dan protokol. Kesulitan yang ada adalah jika terminal beroperasi dengan kecepatan *baud* yang tidak sesuai standar dan jika terminal menggunakan detektor logam maka penggunaan *smartcard* dengan kawat (alat untuk *login*) tidak mungkin dilakukan.
- f. Cari manual. Cara yang paling mudah. Tetapi membutuhkan biaya dan terkadang spesifikasi *smartcard* tidak disebarluaskan ke masyarakat.

Dengan menggunakan spesifikasi terminal kita mengetahui beberapa perintah. Dengan perintah ini kita dapat memilih *file*, dapat membaca data dalam *file*, dapat memperoleh informasi rahasia dan dapat membaca informasi transaksi. Berdasarkan bagaimana cara dan posisi seseorang mendapatkan pesan-pesan dalam saluran komunikasi, penyerangan dapat dikategorikan menjadi:

- a. *Sniffing*: secara harafiah berarti mengendus, tentunya dalam hal ini yang diendus adalah pesan (baik yang belum ataupun sudah dienkripsi) dalam suatu saluran komunikasi. Hal ini umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekap pembicaraan yang terjadi.
- b. *Replay attack*[DHMM96]: Jika seseorang bisa merekam pesan-pesan *handshake* (persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak.
- c. *Spoofing*[DHMM96]: Penyerang – misalnya C – bisa menyamar menjadi A. Semua orang dibuat percaya bahwa C adalah A. Penyerang berusaha meyakinkan pihak-pihak lain bahwa tak ada salah dengan komunikasi yang dilakukan, padahal komunikasi itu dilakukan dengan sang penipu/penyerang. Contohnya jika orang memasukkan PIN ke dalam *Card Acceptance Device* (CAD) – yang benar-benar dibuat seperti CAD asli – tentu sang penipu bisa mendapatkan PIN pemilik *smartcard*. Pemilik *smartcard* tidak tahu bahwa telah terjadi kejahatan.
- d. *Man-in-the-middle*[Schn96]: Jika *spoofing* terkadang hanya menipu satu pihak, maka dalam skenario ini, saat A hendak berkomunikasi dengan B, C di mata A seolah-olah adalah B, dan C dapat pula menipu B sehingga C seolah-olah adalah A. C dapat berkuasa penuh atas jalur komunikasi ini, dan bisa membuat berita fitnah.

Kabel koaksial yang sering digunakan pada jaringan sangat rentan terhadap serangan *vampire tap* yakni perangkat keras sederhana yang bisa menembus bagian dalam kabel koaksial sehingga dapat mengambil data yang mengalir tanpa perlu memutuskan komunikasi data yang sedang berjalan. Seseorang dengan *vampire tap* dan komputer tas (laptop) dapat melakukan serangan pada bagian apa saja dari kabel koaksial. Penyerang juga bisa mendapatkan kunci dengan cara yang lebih tradisional, yakni dengan melakukan penyiksaan, pemerasan, ancaman, atau bisa juga dengan menyogok seseorang yang memiliki kunci itu. Ini adalah cara yang paling ampuh untuk mendapat kunci.

Perencanaan Database Setoran



Gambar 9. Rencana Perangkat Lunak setoran bulanan

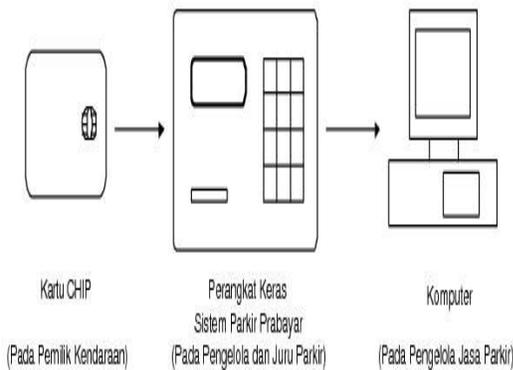
Pada perencanaan Perangkat Lunak ini nantinya akan langsung di inputkan data dari sipengguna jasa perparkiran secara otomatis dalam database. Dan akan tertulis berapa nilai saldo dan sisa saldo yang tinggal.

Field	Tipe	Besar	Keterangan
TGL	DateTime	8	Tanggal Penyetoran
ID	Char	4	Nomor Identitas Alat
SALDO	Currency	10	Jumlah Pendapatan Saldo
HUTANG	Currency	10	Jumlah Pembayaran Tunai

Gambar 10. Field dan tipe data Perangkat Lunak setoran.

C. PEMBAHASAN dan HASIL

Setelah perencanaan dan perancangan diatas dibuat maka selanjutnya adalah tahapan melihat hasil akhir dari perencanaan yang telah dikerjakan. Secara blok diagram dapat dilihat sbb :



Gambar 11. Simulasi dalam bentuk blok diagram perancangan sistem perparkiran.

Dari simulasi berbentuk blok diatas dapat diterangkan bahwa seorang pengguna jasa perparkiran yang telah memiliki identitas kepemilikan dalam sebuah smart card dapat langsung memasukkan identitasnya kedalam card reader. Dari card reader ini akan dibaca dan diteruskan ke computer untuk di verifikasi dan disesuaikan dengan database yang ada. Lalu bila data kepemilikan belum terdapat pada database maka secara otomatis akan ditambahkan.

D. KESIMPULAN

Dari perancangan diatas dapat diraih beberapa kesimpulan yaitu :

1. Smart Card memiliki banyak kegunaan sebagai media storage untuk menyimpan identitas kepemilikan
2. Sistem retribusi perparkiran yang dirancang bersifat umum, artinya dapat disesuaikan dengan kebutuhan pengelola jasa perparkiran.
3. Mikrokontroler AT89C52 memiliki keunikan tersendiri yaitu mampu melakukan komunikasi dengan beberapa perangkat sekaligus. Dan memiliki kapasitas penyimpanan data yang cukup besar.

DAFTAR PUSTAKA

- Ariyus, Dony. 2005, *Computer Security*, Penerbit Andi, Jogjakarta
- Den, Heijer P.C et al, 1991, *Komunikasi Data*, Elex Media Komputindo
- Saydam, Gouzali. 1993, *Sistem Telekomunikasi*, Djambatan
- Syafrizal, Melwin. 2005, *Pengantar Jaringan Komputer*, Penerbit Andi, Jogjakarta

Penulis

1. **Abdul Jabbar Lubis**
2. **Evri Ekadiansyah**

Staf Pengajar

STMIK POTENSI UTAMA MEDAN

Halaman ini sengaja dikosongkan