JAVA RING

A Seminar Report

Submitted by

AJAY GUPTA

in partial fullfillment for the award of degree of

Bachelor of Technology (B.Tech.)

in

Information Technology

Department of Computer Engineering
Malaviya National Institute of Technology,Jaipur

March,2011

Submitted To:
Mr.Girdhari Singh

Mentor:
Mrs. Namita Mittal

MALAVIYA NATIONAL INSTITUTE OF TECHNOLOGY

(DEEMED UNIVERSITY)

Jaipur-302017(RAJ.)

DEPARTMENT OF COMPUTER ENGINEERING

CERTIFICATE

This is to certify that the seminar report entitled

JAVA RING

Which is being submitted by

AJAY GUPTA

In partial fulfillment of degree of Bachelor of Technology in Information Technology from Malaviya National Institute of Technology Jaipur.
This seminar report has been found to be quite satisfactory and is approved for submission.

Date:

Mrs.Namita Mittal
Assistant Professor
(Computer Engg. Dept.)

ACKNOWLEDGEMENT

Many people have contributed to the success of this. Although a single sentence hardly suffices, I would like to thank Almighty God for blessing me with His grace. I extend my sincere and heartfelt thanks to **Mr. Girdhari Singh**, Assistant Professor Computer Engineering Department, for providing me the right ambience for carrying out this work. I am profoundly indebted to my seminar guide **Mrs. Namita Mittal**, Assistant Professor Computer Engineering Department for innumerable acts of timely advice,encouragement and I sincerely express my gratitude to her. I express my immense pleasure and thankfulness to all the teachers and staff of the Department of Computer Science for their cooperation and support. Last but not the least, I thank all others, and especially my classmates who in one way or another helped me in the successful completion of this work.

AJAY GUPTA

Contents

List of Figures

ABSTRACT

A Java Ring is a finger ring that contains a small microprocessor with built-in capabilities for the user, a sort of smart card that is wearable on a finger. Sun Microsystemś Java Ring was introduced at their JavaOne Conference in 1998 and, instead of a gemstone, contained an inexpensive microprocessor in a stainless-steel iButton running a Java virtual machine and preloaded with applets (little application programs)[9].

The rings were built by Dallas Semiconductor.Workstations at the conference had ring readers installed on them that downloaded information about the user from the conference registration system. This information was then used to enable a number of personalized services. For example, a robotic machine made coffee according to user preferences, which it downloaded when they snapped the ring into another ring reader[3].

The Java Ring is an extremely secure Java-powered electronic token with a continuously running, unalterable real-time clock and rugged packaging, suitable for many applications. The jewel of the Java Ring is the Java iButton – a one-million transistor, single chip trusted microcomputer with a powerful Java Virtual Machine (JVM) housed in a rugged and secure stainless-steel case[9].

The Java Ring is a stainless-steel ring, 16-millimeters (0.6 inches) in diameter, that houses a 1-million-transistor processor, called an iButton.The ring has 134 KB of RAM, 32 KB of ROM, a Real-time clock and a Java virtual machine, which is a piece of software that recognizes the Java language and translates it for the userś computer system[3].

Designed to be fully compatible with the Java Card 2.0 standard the processor features a high-speed 1024-bit modular exponentiator for RSA encryption, large RAM and ROM memory capacity, and an unalterable Real time clock. The packaged module has only a single electric contact and a ground return, conforming to the specifications of the Dallas Semiconductor 1-Wire bus. Lithium-backed Non-Volatile SRAM offers high read/write speed and unparallel tamper resistance through near-instantaneous clearing of all memory when tampering is detected, a feature known as rapid zeroization[3].

Chapter 1

INTRODUCTION-A PORTABLE WEARABLE COMPUTER

It seems that everything we access today is under lock and key. Even the devices we use are protected by passwords. It can be frustrating trying to keep with all of the passwords and keys needed to access any door or computer program[4].

Dallas Semiconductor is developing a new Java- based, computerized ring that will automatically unlock doors and log on to computers.

In the domain of identification traditional technologies are used, such as the bar codes applied on surfaces, the magnetic stripes, the chip cards, and the RFID labels. To these technologies can be added another successful one, which is based on the 1-wire communication network[14].

The 1-wire technology has emerged from the evolution of the semiconductor technology. It was designated to some specific applications to substitute the identification by paper label based on bar codes for the electronic circuits. Dallas Semiconductor was the first producer which developed a large used automated identification through attached chips to objects or persons[14].

The iButton technology belongs to the category of the technologies of identification by touching. The simplest identification method can be realized by using a microsystem with two external electrical wire connexions: signal and ground[14].

This mobile computer can become even more secure. You can keep the iButton with you wherever you go by wearing it as a closely guarded accessory - a watch, a key chain, a wallet, a ring - something you have spend your entire life practicing how not to lose.

Here are a few reasons why you might want to wear the iButton in the accessory that best fits your life style:

- It is a safe place to keep the private keys to conduct transactions.
- It overcomes the deficiencies of the secret password.
- You eliminate keystroke with a quick, intentional press of the Blue Dot.
- You keep your computer at hand versus lugging your everywhere you roam.
- You become part of the network economy.
- The reading without expensive optical devices.
- Reading and Writing are done by means of small-sized portable having a reduced energy consumption.
- The hundredfold increased storage of data as compared to a bar code.
- The identification through a unique serial number (which can represent a node in a global network of a practically unlimited dimension).
- It has multifunctionality by integrating, into the same device, another functions (temperature and humidity sensors, etc.)
- The content of the iButton chip can be modified while it is attached to the object, it can allow over 1 milion programming cycles of EEPROM memory.
- This steel-bound credential stands up to the hard knocks of everyday wear, including sessions in the swimming pool or clothes washer[14].

Figure 1.1: Prototype of stainless steel java ring[11]

Chapter 2

HISTORICAL BACKGROUND

In the summer of 1989, Dallas Semiconductor Corp. produced the first stainless-steel-encapsulated memory devices utilizing the Dallas Semiconductor 1-Wire communication protocol. By 1990, this protocol had been refined and employed in a variety of self contained memory devices[3].

Originally called “touch memory” devices, they were later renamed “iButtons”. Packaged like batteries, iButtons have only a single electrical contact on the top surface, with the stainless steel shell serving as ground. The now famous Java Rings made their appearance at the conference (March 24-27), issued to attendees when they picked up their materials at registration. With one of these rings a user could communicate with the computers at the Hackers' Lab, help build a large fractal image at the show, or even get a cup of his or her favorite coffee[3].

Built by Dallas Semiconductor, the durable, wearable Java Ring is practically indestructible but not heavy or clumsy. The jewel of the ring is a relatively inexpensive device called an iButton, which contains a processor that runs a Java Virtual Machine.

At the conference, the Java Rings were preloaded with applets that could communicate with corresponding host applications on various networked systems installed at the show.

The first time an attendee snapped the ring's iButton into a ring reader attached to a workstation, an applet on the ring communicated with the host application on the system. The applet in turn downloaded the user's personal information from the conference registration system and allowed the user to select their preferred type of coffee (a process they called "personalizing" the ring). From there, the user could walk over to a "coffee factory," snap the ring into another reader, and the robotic coffee machine would make the brew based on the user's preference stored in the ring.

Data can be read from or written to the memory serially through a simple and inexpensive RS232C serial port adapter, which also supplies the power required to perform the I/O. The iButton memory can be read or written with a momentary contact to the "Blue Dot" receptor provided by the adapter. When not connected to the serial port adapter, memory data is maintained in Non-Volatile Random Access Memory (NVRAM) by a lifetime lithium energy supply that will maintain the memory content for at least 10 years[3].

Unlike Electrically Erasable Programmable Read-Only Memory (EEPROM), the NVRAM iButton memory can be erased and rewritten as often as necessary without wearing out. It can also be erased or rewritten at the high speeds typical of Complementary Metal Oxide Semiconductor (CMOS) memory, without requiring the time-consuming programming of EEPROM.

For those who attended the 1998 Java One Developer Conference at the Moscone Center in San Francisco last spring, the Java Ring was arguably the jewel in the crown of the four-day gathering. No other facility garnered quite such excitement, enthusiasm, and overall industry buzz. There were simply no bigger lines to be had than those to obtain the rings, to "personalize" them, and then to play the ring-based fractal game and enjoy a ring-driven respite of custom brewed coffee.

Chapter 3

JAVA RING

3.1 What is Java Ring?

The Java Ring is a stainless-steel ring, 16-millimeters (0.6 inches) in diameter that houses a 1-million-transistor processor, called an iButton. The ring has 134 KB of RAM, 32 KB of ROM, a real-time clock and a Java virtual machine, which is a piece of software that recognizes the Java language and translates it for the user's computer system[4].

At Celebration School, the rings have been programmed to store electronic cash to pay for lunches, automatically unlock doors, take attendance, store a student's medical information and allow students to check out books. All of his information is stored on the ring's iButton. Students simply press the signet of their Java ring against the Blue Dot receptor, and the system connected to the receptor performs the function that the applet instructs it to[4].

In the future, the Java Ring may start your car. Mobile computing is beginning to break the chains that tie us to our desks, but many of today's mobile devices can still be a bit awkward to carry around. In the next age of computing, we will see an explosion of computer parts across our bodies, rather than across our desktops[4].

Digital jewelry, designed to supplement the personal computer, will be the evolution in digital technology that makes computer elements entirely compatible with the human form. The Java Ring, first introduced at Java One Conference, has been tested at Celebration School, an innovative K-12 school just outside Orlando; FL. The rings given to students are programmed with Java applets that communicate with host applications on networked systems. Applets are small applications that are designed to be run within another application. The Java Ring is snapped into a reader, called a Blue Dot receptor, to allow communication between a host system and the Java[4].

3.2 Insight to Java Ring

The world today is in hunt for the new technology, and has contributed miracles to the field of science, the ever ending stream. The one such contribution is the JAVA RING, a finger ring that contains a small microprocessor with built-in capabilities for the user, a sort of smart card that is wearable on a finger. Well it's something new to the world. Since it has not been very popular these days, it's really a new opening for sure[11].

Introducing more of it, we can say that, it contains an inexpensive microprocessor in a stainless steel iButton, this particular ring is running on a Java Virtual Machine and it is preloaded with applets. Java virtual machine as we all knows[11].

The JVM is the "processor architecture" on which java byte code is executed. It is mostly implemented in software, and available for a large variety of hardware platforms, ranging from mainframe computers to mobile phones and small embedded devices[11].

3.3 Operating System in Java Ring

A special operating system was designed and stored in the ROM of the Crypto iButton to support cryptography and general-purpose financial transactions – such as those required by the Postal Service program. While not a Java virtual machine, the E-Commerce firmware designed for this application had several points of similarity with Java, including an object- oriented design and a byte code interpreter to interpret and execute Dallas Semiconductor's custom-designed E-Commerce Script Language[3].

A Compiler was also written to compile the high-level language representation of the Script Language to a byte code form that could be interpreted by the E-Commerce VM.

Although the E-Commerce firmware was intended primarily for the USPS application, the firmware supports a variety of general electronic commerce models that are suitable for many different applications. The E-Commerce firmware also supports cryptographic Protocols for secure information exchange such as the Simple Key- Management for Internet Protocol (SKIP) developed by Sun Microsystems Inc[3].

3.4 Security

National Institute of Standards and Technology (NIST) and the Canadian Security Establishment (CSE) have validated the DS1954 Cryptographic iButton as meeting Federal Information Processing Standards Publications (FIPS PUBS) 140-1, "Security Requirements for Cryptographic Modules" (FIPS 140-1)[13].

The Crypto iButton includes the highest level of physical security ever validated by the FIPS 140-1 program, and it does this in an extremely small and durable package. There is no other hardware token like this, meeting government and federal requirements and providing rich functionality at a fraction of the cost of similar devices[13].

The Crypto iButton provides hardware cryptographic services such as long-term safe storage of private keys, a high-speed math accelerator for 1024- bit public key cryptography, and secure message digest (hashing).

The Crypto iButton consists of a physically secure, million-transistor microchip packaged in a 16mm stainless steel can. Not only does the steel protect the silicon chip inside from the hard knocks of everyday use, it also shows clear evidence of tampering by leaving scratch and dent marks of the intruder[7].

This steel case satisfies FIPS 140-1 Level 2 Tamper Evidence requirements for physical security[7].

Additional physical security measures designed into the Crypto iButton meet the FIPS 140-1 Level 3 Tamper Response requirements. If the steel case is opened, a microswitch triggers a tamper response, which results in rapid zeroization of the chip's contents, destroying private keys and other sensitive information[7].

The iButton constantly monitors the switch's contacts, and any separation of the cryptographic chip from the lithium cell returns the device to on-chip capacitor power to perform a complete zeroization as its last powered action. Orchestrated attacks to uncover iButton secret information by subjecting it to extreme temperature or voltage conditions will also generate a tamper response that results in zeroization[7].

Deliberate exposure to temperatures outside the iButton's operational range of minus 20 degrees C to 70 degrees C (minus 4 degrees F to 158 degrees F) causes temperature monitors to trigger a cold- or high-temp response that quickly erases (zeroes) the memory contents. This feature allows the iButton to meet the FIPS 140-1 Level 4 Environmental Failure Protection (EFP) requirements[7].

If an excessive voltage is applied to the sole I/O pin, an electronic fuse renders the chip inoperable to protect the chip from out-of-spec voltage stresses[13].

The barrier substrate and the triple layer technique effectively deny access the unauthorized access to the NVRAM confidential data. In the worst case if any unauthorized access penetrates the barrier the security processor detects it and immediately the data which is written in the NVRAM. The Crypto iButton hardware platform offers a unique set of special features expressly designed to prevent private keys and other confidential information from becoming available to hackers[13].

Individuals maintain control over their Crypto iButton in yet another way secret "Personal Identification Numbers". If so programmed, the iButton will not perform computations until its PIN is entered, like a bank ATM[7].

Chapter 4

COMPONENTS

The main components of java ring are following:-

- Java Virtual Machine (JVM)
- RAM
- ROM
- Real Time Clock
- IButton
- Blue Dot Receptor
- 1-Wire Interface

4.1 Java Virtual Machine(JVM)

Java ring is programmed with java application program and applets that communicate with the host application on the networked system. Applets are the small application that is designed to run on the application system. The java virtual machine is the piece of software that recognizes the java language and translates the byte code, which is used by the system which is connected to the java ring via ring reader.

At Celebration School, the rings have been programmed to store electronic cash to pay for lunches, automatically unlock doors, take attendance, store a student's medical information and allow students to check out books. All of this information is stored on the ring's iButton. Students simply press the signet of their Java Ring against the Blue Dot receptor, and the system connected to the receptor performs the function that the applet instructs it to. In the future, the Java Ring may start your car[4].

4.2 RAM

Java ring contains 134kb of Non-Volatile Random Access Memory(NVRAM). Program and data is stored in this NVRAM .This Non-Volatile Random Access Memory offers high read/write speed and also provides temper resistance through instantaneous clearing of all memory when tempering is detected. This process is called rapid zeroization. The NVRAM iButton memory can be erased or rewritten as often as necessary without wearing out. High security is offered by the ability to erase the content of NVRAM extremely quickly[5].

The Crypto iButton also provides an excellent hardware platform for executing Java because it utilizes NVRAM for program and data storage. With 6 kilobytes of existing NVRAM and the potential to expand the NVRAM capacity to as much as 128 kilobytes in the existing iButton form factor, the Crypto iButton can execute Java with a relatively large Java stack situated in NVRAM.

This memory acts as conventional high-speed RAM when the processor is executing, and the lithium energy preserves the complete state of the machine while the Java Ring is disconnected from the reader. There is therefore no requirement to deal with persistent objects in a special way – objects persist or not depending on their scope so the programmer has complete control over object persistence.

As in standard Java, the Java iButton contains a garbage collector that collects any objects that are out of scope and recycles the memory for future use. Applets can be loaded and unloaded from the Java iButton as often as needed. All the applets currently loaded in a Java iButton are effectively executing at zero speed any time the iButton is not in contact with a Blue Dot receptor . As the Java Card 2.0 specification was proposed, Dallas Semiconductor became a Java Soft licensee. The agreement called for the development of a Java Card 2.0 implementation and also for the design of "plus portions" that take advantage of the unique capabilities afforded by the Crypto iButtons NVRAM, such as the ability to support a true Java stack and garbage collection. With the addition of the continuously running lithium-powered time-of- day clock and the high- speed, large-integer modular exponentiation engine.

4.3 ROM

The java ring contains 32kb of ROM .A special kind of operating system called E - Commerce operating system which is based on java and JVM is stored in the ROM.This operating system handles all the operation which is happening in the iButton. It is stored in ROM because it is not supposed to be altered by the user. The Crypto iButton hardware platform offers a unique set of special features expressly designed to prevent private keys and other confidential information from

becoming available to hackers[5].

A32-kilohertz crystal oscillator is used in the Java iButton to operate the time-of-day clock at a constant and well-controlled frequency that is independent of the processor clock[3].

4.4 Real Time Clock

In the java ring real time clock gives the exact time of the day. The real time clock continuously running up to more than 10 years by the energy provided the lithium backup.

A 32-kilohertz crystal oscillator is used in the Java iButton to operate the time-of-day clock at a constant and well-controlled frequency that is independent of the processor clock[3].

In addition, the processor itself is driven by an unstabilized ring oscillator operating over a range of 10 to 20 megahertz, so that the clock frequency of the processor is not constant and cannot be determined by external means. This differs from the design of alternative devices in which the processor clock signal is injected by the reader and is therefore exactly determined by the host processor.

External control of the clock provides a valuable tool to hackers, since they can repetitively cycle such a processor to the same point in its execution simply by applying the same number of clock cycles. Control of the clock also affords a means to induce a calculation error and thereby obtain information that can ultimately reveal secret encryption keys. A 32-kilohertz crystal oscillator is used in the Java iButton to operate the time-of-day clock at a constant and well-controlled frequency that is independent of the processor clock[3].

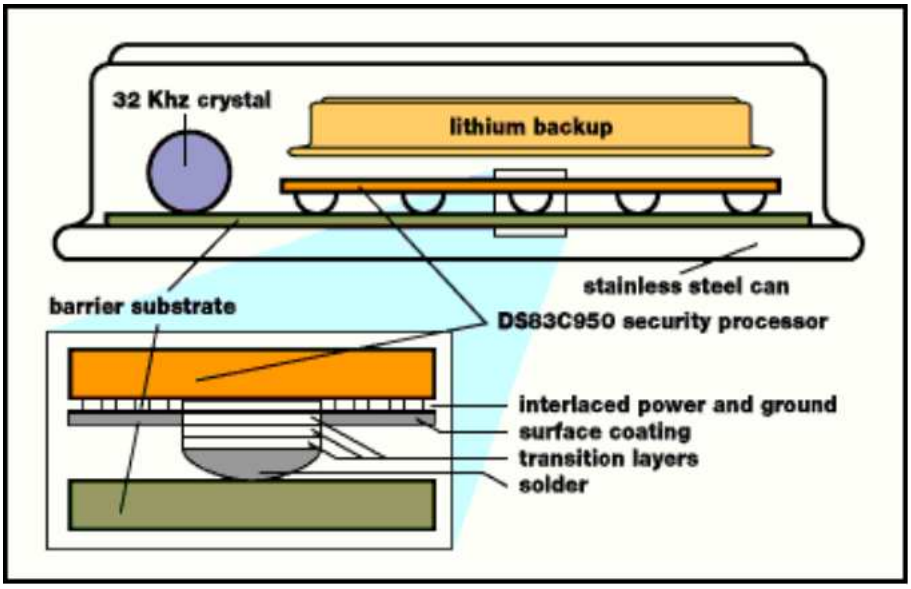

Figure 4.1: Internal construction of the iButton[11]

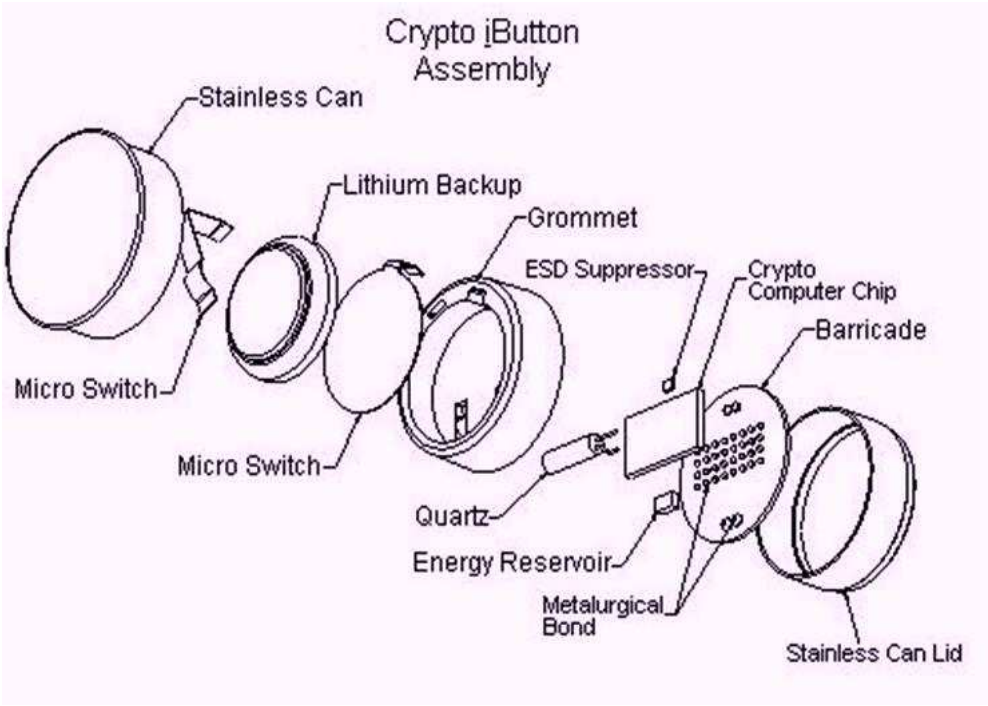

Figure 4.2: Components of the DS1954B Crypto iButton[15]

4.5 IButton

The jewel of the java ring is the java iButton .It contains one million transistor processor single chip trusted microprocessor with powerful Java Virtual Machine(JVM) housed in rugged and secure stainless steel case. The Crypto iButton hardware platform offers a unique set of special features expressly designed to prevent private keys and other confidential information from becoming available to

hackers[1].

Figure 4.1 shows a detail of the internal construction of the Crypto iButton. The silicon die containing the processor, ROM, and NVRAM memory is metallurgically bonded to the barrier substrate through which all electrical contacts are made. This barrier substrate and the triple-layer metal construction techniques employed in the silicon fabrication effectively deny access to the data stored in the NVRAM. If any attempt is made to penetrate these barriers, the NVRAM data is immediately erased[3].

Figure 4.3: Different types of iButtons available in the market[1]

This construction technique and the use of NVRAM for the storage of private keys and other confidential data provides a much higher degree of data security than that afforded by EEPROM memory. The fact that the communication path between the Crypto iButton and the outside world is limited to a single data line provides additional security against hardware attacks by limiting the range of signals accessible to the hacker[3].

It is originally called touch memory devices they were later renamed as "iButtons packaged" like batteries. IButton have only a single active electrical contact on the top surface and with the stainless steel shell serving as ground. Every iButton product is manufactured with unique 8 byte serial number and carries a guaranty that no two IButtons have same number. Among the simplest iButton are memory devices which can hold files and directories that can be read and written like small floppy disks.

An iButton is a microchip similar to those used in smart card but housed in a round stainless steel button of 17.35mm x 3.1mm - 5.89mm in size (depending on the function). The iButton was invented and is still manufactured exclusively by Dallas Semiconductor mainly for applications in harsh and demanding environments.

Like a smart card, an iButton does not have an internal power source. It requires connection to a reader (known as a Blue Dot Receptor) in order to be supplied with power and to receive input and send output. Unlike some smart cards, there are currently no contactless iButtons: they require physical contact with a reader to function.

There are iButtons that measure temperature (for food storage and transport); have an electronic ID (for physical access to buildings); and store e-cash (for purchases both in stores and via the web). For e- commerce applications, the iButton can support Java Card 2.0/OpenCard standards in addition to proprietary software.

iButtons have an advantage over conventional smart cards in term of durability and longevity. The stainless steel casing gives iButton a far greater ability to survive in a range of temperatures – all versions are functional from -40 C to +70 C – and in a much harsher range of environments (such as exposure to salt water and long term exposure to physical impacts) than the plastic smart card. For e-commerce and personal ID usage, iButtons can be mounted on a range of personal accessories: watch, ring, key chain, or dog tag.

4.5.1 Types of Ibutton

There are multiple different iButtons available. Each starts with a guaranteed-unique registration number engraved in the silicon. From there, iButtons branch out into three different types[5]:

Memory iButton

64K and beyond of computer memory stores typed text or digitized photos. Information can be updated as often as needed with a simple, momentary contact. Some memory iButtons contain a real-time clock to track the number of hours a system is turned on for maintenance and warranty purposes (DS1994); a temperature sensor for applications where spoilage is a concern, such as food transport (DS1921); or a transaction counter that allows the iButton to be used as a small change purse (DS1963).

Java-powered cryptographic iButton

A microprocessor and high-speed arithmetic accelerator generate the large numbers needed to encrypt and decrypt information. The Java-powered iButton adds its complete cryptographic circuitry to a Java Virtual Machine (VM) that is Java CardTM 2.0-compliant, enabling the world's large pool of Java programmers to tap into a powerful development tools to get an application up and running quickly.

The Java-powered iButton's greatest promise lies in its capacity to interact with Internet applications to support strong remote authentication and remotely authorized financial transactions. In practical terms,that means you can jump into the age of electronic commerce with both feet: your messages are sent over the Internet scrambled and can only be unscrambled at the other end by someone with an authorized iButton. By establishing a means to transmit and protect user identity, the iButton becomes the user's digital credential.

Thermochron iButton

This iButton tracks time and temperature, keys to the freshness of many products. The Thermochron integrates a thermometer, a clock/calendar, a thermal history log, and 512 bytes of additional memory to store a shipping manifest.

Figure 4.4: Difference types of blue dot receptor in the market[1]

4.6 1-Wire Interface

By simply touching each of the two contacts we can communicate to any of the iButtons by using 1-Wire protocol. The 1-Wire interface has two communication speeds. Standard mode is at 16kbps and overdrive mode at 12kbps. 1-wire protocol is used for communication between PC and the blue dot receptor over the 1-wire Network. 1-Wire Network includes a system with a controlling software, wiring and connectors and iButtons[1].

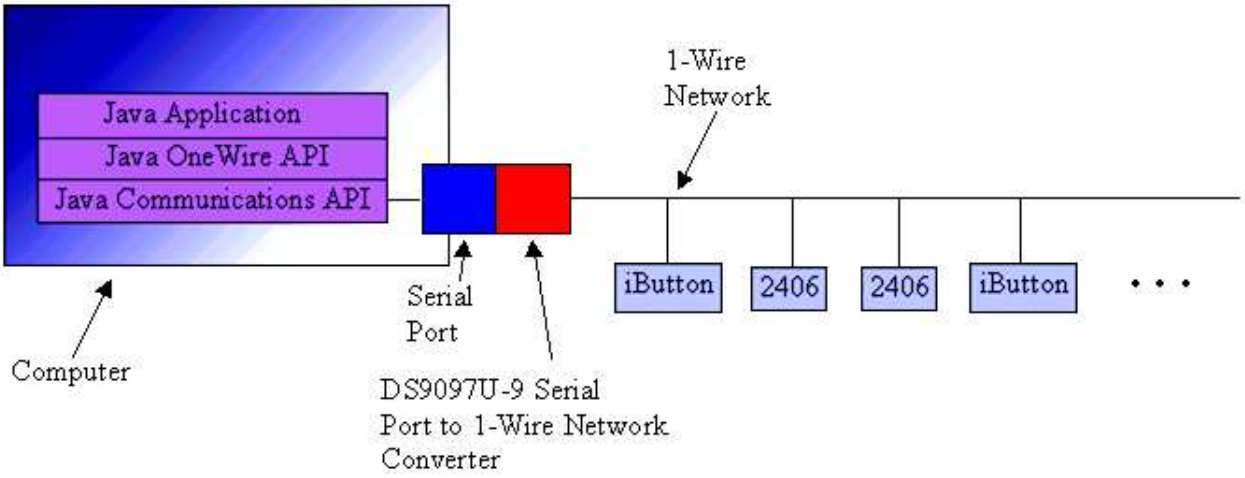

Figure 4.5: 1-wire Network[2]

The Dallas Semiconductor 1-Wire bus is a simple signaling scheme that performs two-way communications between a single master and peripheral devices over a single connection. A powerful feature that all 1-Wire bus devices share is that each and every device, in a chip or an iButton, has a factory-lasered serial number that will never be repeated in any other device. That is to say, every device is unique.

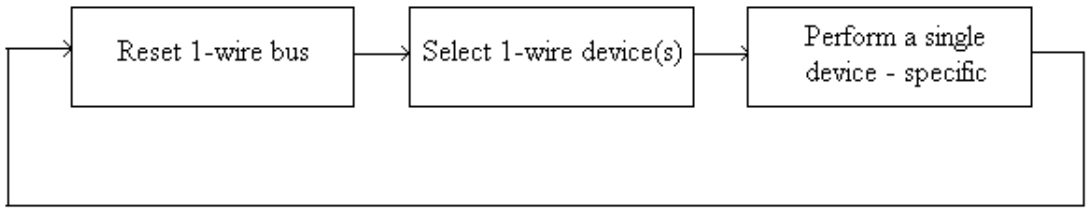

Figure 4.6: 1-Wire Interface[2]

This allows any single device to be individually selected from among many that can be connected to the same bus wire. Because one, two, or even dozens of 1-Wire devices can share a single wire for communications, a binary searching algorithm is used to find each device in turn. Once each device serial number is known, any device can be uniquely selected for communication using that serial number to address it[6].

The first part of any communication involves the bus master issuing a "reset" which synchronizes the entire bus. A slave device is then selected for subsequent communications. This can be done by selecting all slaves, selecting a specific slave (using the serial number of the device), or by discovering the next slave on the bus using a binary search algorithm. These commands are referred to collectively as "network" or ROM (Read-Only-Memory) commands.

Once a specific device has been selected, all other devices drop out and ignore subsequent communications until the next reset is issued. Once a device is isolated for bus communication the master can issue device-specific commands to it, send data to it, or read data from it. Because each device type performs different functions and serves a different purpose, each has a unique protocol once it has been selected. Even though each device type may have different protocols and features, they all have the same selection process and follow the command as per the requirements.

An integral part of the unique serial number in each slave is an 8-bit family code. This code is specific to the device model. Because each device model performs different functions, this code is used to select the protocol that will be used to control or interrogate it. Reset 1-Wire bus Select 1-Wire device(s) perform a single device- specific operation.

The Address:

Each iButton has a unique and unalterable address that is laser etched onto its chip inside the can. The address can be used as a key or identifier for each iButton[1].

2700000095C33108

From these basics we have expanded the iButton product line into over 20 different products by adding different functionality to the basic button. Dallas Semiconductor's 1-Wire devices each have a 64-bit unique registration number in read-only-memory (ROM) that is used to address them individually by a 1-Wire master in a 1-Wire network. If the ROM numbers of the slave devices on the 1-Wire network are not known, then they can be discovered by using a search algorithm.

64-Bit Unique ROM 'Registration' Number:

MSB 64 'Registration 'ROM Number LSB		
8 bit CRC	48-bit Serial	8-bit Family Code

The memory map for the 64-bit number occupies three sections each serving a slightly different purpose when read by a host processor. The first 8 bits identify the iButton's product family, information that the host requires to access different kinds of networked iButtons using the 1-Wire protocol. The middle 48 bits constitute the digitally unique serial number. The last 8 bits are CRC code that the host can use to verify error-free reading[14].

The iButton communicates with a processor using 1-Wire protocol through a hardware port interface. The port interface provides both the physical link and handles the communication protocols that enable the processor to access iButton resources with simple commands.

4.7 Tmex Runtime Environment (TRTE)

A layer of software is required to interface iButtons to computers and produce the desired information in the desired format. For all iButtons, iButton- TMEX is a software platform on which to build applications. TMEX removes the tedious low-level programming of drivers and utilities.

The TRTE installs the drivers and demo software for all iButtons and 1- Wire devices. TMEX's architecture follows the International Standards Organization (ISO) reference model of Open System Interconnection (OSI), a protocol with seven layers denoted as Physical, Link, Network, Transport, Session, Presentation, and Application. The current release of TMEX RTE supports Microsoft 32-bit Windows. This includes Windows Me, 2000, 98, 95, NT 4.00, and NT 3.51.

Chapter 5

WORKING OF JAVA RING

Since java ring is programmed with the applets and the programming is done according to our application and this will specific for the specific user. All information of the user is stored in the java ring[11].

Figure 5.1 shows how java ring is used to open the door. User simply has to press the signet of the java ring against the blue dot receptor and the system connected to the receptor performs the function that the applets instruct it to.java ring has the user profile and the same profile is present in the door embedded

Figure 5.1: Opening door using Java Ring[1]

system also, when the user press the signet of the java ring against the java ring reader which is embedded at the handle of the door the data is transferred from the ring to door system. if the profile is authentic means user is authentic to open the door the applets president in the ring instruct the door to open.

Information is transferred between iButton and a PC with a momentary contact, at up to 142K bits per second. To do that one presses iButton to the Blue Dot receptor, a 15 pipeline into PC. The Blue Dot sticks to any convenient spot on the front of a PC and is cabled to the serial or parallel port in the back[1].

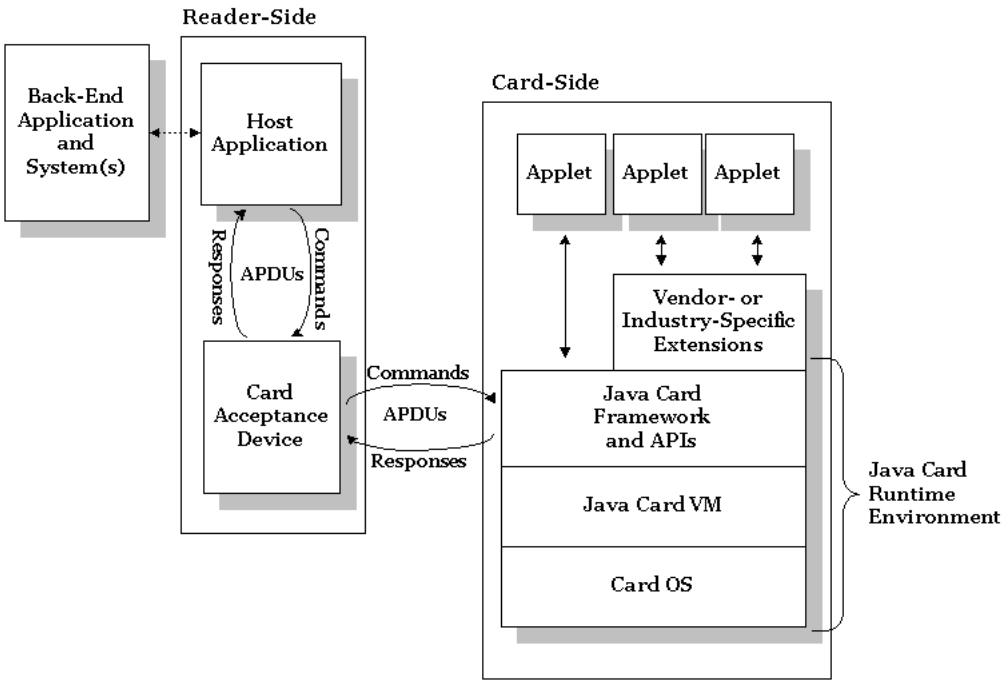

Figure 5.2: Working process of Java Ring(Source:Java Card Technology)

According to the Dallas Superconductor's information, over 41 million iButtons are currently in circulation. List of the major users include the U.S. Post Office, entire truck fleet fitted with iButtons that track vehicle maintenance; Citizens of Istanbul, Turkey, who store digital cash in the iButton, using the device as a small change purse on their mass transit system. It was also said that the U.S. Postal service has approved.

Chapter 6

APPLICATIONS

The iButton is ideal for any application where information needs to travel with a person or object. Affixed to a badge, key fob, watch, or ring, an iButton can grant its owner access to a building, a PC, a piece of equipment, or a vehicle. Attached to a work tote, it can measure a variety of processes to improve efficiency, such as manufacturing, delivery, and maintenance[12].

Some versions of the iButton can be used to store cash for small transactions, such as transit systems, parking lots, and vending machines. The iButton can also be used as an electronic asset tag to store information needed to keep track of valuable capital equipment.

The java ring is used initially as rugged portable data carriers. Often in harsh environmental condition. It is used for many real world application e.g. for opening the door ,in the e-banking application for getting the balance in your account. Logging in your personal computer. Providing security in your car.

This demonstration shows how an e-banking application (Jini client)tries to connect to a bank server (Jini service) to retrieve the current account balance of that user.

Figure 6.1: Application of java ring for getting account balance of a user through internet[1]

Since all bank data must be treated confidential, the bank server interacts with the security infrastructure that is installed at the bank, before it responds to the application. The bank's security infrastructure demands that the user must authenticate herself to get the permission. Therefore an authentication scheme is started at user side that asks the user to push her Java Ring on the Java Ring reader. Inside the Java Ring resides a Java interpreter that executes cryptographic routines to perform that task. After the authentication process on the Java Ring, the bank knows the identity of the user and that she is really the one, she pretends to be. Then the bank service can send the confidential and personalized data to the e-banking application that displays the current account balance[12].

Other Important Applications are:-

- Opening the door
- Electronic access control
- Asset management
- E cash
- Guard tour
- Configuring car component according to preferences

Chapter 7

ADVANTAGES AND DISADVANTAGES

7.1 Advantages

The Java Ring is ideal for applications where information needs to travel with a person or object. It replaces many memory devices that can hold files and subdirectories and can be read and written like small floppy disks.

It can also replaces many password protected devices that are used for financial transaction, point-of-sales transactions, remote access authorization, data logging , maintenance, and quality control.

It has the potential to replace coins, paper money, credit card and other identification card. Since the rings can been programmed to store electronic cash, automatically unlock doors, store a medical information and other personal information.

Also, Java Ring with the iButton can overcome the deficiencies of the secret passwords or pin number. It can be used to store the secret passwords and private keys needed to conduct a transaction. Using the Java Ring, the keystrokes can be eliminated with a quick press of the Blue Dot[6].

Internet services like e-banking or door opener can be secured and personalized without entering the name and password.

Another Important Advantages are:-

- Clam-shell steel container, the Micro can is suitable for harsh environments.
- Multiple iButtons sharing the same conductive surface can be read or written individually by the same contact.

- Provides authentication to users which is crucial for many applications.
- Provides real memory and more power.
- Java Ring do not need radio frequencies, since data is transferred by electrical conductivity during the momentary contact. this allow their use without any license in every country[6].

7.2 Disadvantages

Although, Java Ring can be the most secure storage medium for many industries, the cost of implementing the system could be very high. Even though ibutton can be purchased for cheaper price, in order to function, it needs a receiver such as blue dot receptor which could be very Expensive[9].

Also, it needs a high level tools and method in order to program application efficiently, reliably, securely.

A Java Ring-based system doesn't automatically allow user mobility. The problem with the Java Ring that many of the organization don't even know the existence of Java Ring. User mobility is only possible if every machine that the user access has an iButton reader attached. The machine must support the same standard ibutton reader interfaces or use the same proprietary iButton reader[9].

IButton has a limited processor power and memory. For better performance and scalability it is imperative to move the processing load to the application server. Also only limited amount of information can be stored which means an individual might need to carry more than one Java Ring. Carrying the Java Ring everywhere could lead to theft issues.

Chapter 8

CONCLUSION

Java ring is highly durable because of its rugged and secure stainless packing. Dallas Semiconductor has produced more than 20 million physically-secure memories and computers with hard-shell packaging optimized for personal session[3].

The Java iButton, therefore, is simply the latest and most complex descendant of a long line of products that have proven they to be highly successful in the marketplace. With its stainless steel armor, it offers the most durable packaging for a class of products that likely will suffer heavy use and abuse as personal possessions[3].

The iButton form factor permits attachment to a wide variety of personal accessories that includes rings, watchbands, key fobs, wallets, bracelets, and necklace , so the user can select a variation that suits his or her lifestyle[3].

While the Java iButton can readily support the commerce models that have traditionally been the province of credit cards, its greatest promise appears to lie in its capacity to interact with Internet applications to support strong remote authentication and remotely authorized financial transactions. The use of Java promotes compatibility with these applications by providing a common language for all application programming[3].

Bibliography

[1] http://www.maxim-ic.com/products/ibutton/ibuttons

[2] http://www.maxim-ic.com/products/1-wire/flash/overview/index.cfm

[3] http://www.javaworld.com/javaworld/jw-04-1998/jw-04-javadev.html

[4] http://electronics.howstuffworks.com/gadgets/home/digital-jewelry4.htm

[5] http://www.123eng.com/forum/viewtopic.php?p=158456

[6] pdfserv.maxim-ic.com/en/an/AN937.pdf

[7] http://findarticles.com/p/articles/mi_m0EIN/is_1998_July_21/ai_20924045/?tag=content;col1

[8] http://en.wikipedia.org/wiki/1-Wire

[9] http://javaring.blogspot.com/

[10] http://www.maxim-ic.com/products/ibutton/software/crypto/fips140-1l3.pdf

[11] http://hubpages.com/hub/JAVA-RING–INTRODUCING-THE-LATEST-FINGER-RING-PROCESSOR

[12] http://www.maxim-ic.com/products/ibutton/applications/

[13] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION (Supercedes FIPS PUB 140-1, 1994 January 11)

[14] An Identifying and Authorizing Application Using 1-Wire Technology(2010 IEEE 16th International Symposium for Design and Technology in Electronic Packaging (SIITME))

[15] FIPS 140-1 Non-Proprietary Cryptographic Module Security Policy Level 3 Validation (August 2000)