Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

IJMTER

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

Raspberry Pi Based RC4 Encryption Algorithm Implementation for Secure Sensor Node

Mr. Rajendra Babu Medisetti [1] ,Ms. Miti joshi[2]

[1]*M.Tech, Department of ECE, JNTU (Anantapur), Andhra Pradesh, India*

[2]*M.Tech, Seer Academy, Andhra Pradesh, India*

Abstract—Sensor networks are expected to play an essential role in the upcoming age of pervasive computing. Due to their constraints in computation, memory, and power resources, their susceptibility to physical capture, and use of wireless communications, security is a challenge in these networks. The scale of deployments of wireless sensor networks require careful decisions and trade-offs among various security measures Since there is an increase in possible software attacks on privacy and safety of health applications, safety and reliability of the sensor data is an important issue that needs to be addressed in this field. A unique design of a secure sensor node prototype has been proposed and implemented.

In this prototype we using the PCF8591 module this is used for converting Analog to digital data for Raspberry Pi. By using th is we communicate both modules as a Master and Slaves for I2C protocol. With help of I2C we can collect the data from sensors like LDR, Temperature sensors and then this data will be saved in a readable and writeable format in directory like VAR (Variable data stored by daemons and utilities) and then this data will encrypted with RC4 algorithm and similarly the encrypted data will be decrypted by RC4 algorithm by key sent by user by using HTML page from an Embedded server that was installed in raspberry Pi both in desktop and mobile platforms the secure sensor data will be display on monitor with QT farmed environment.

Index Terms— Raspberry pi, PCF8591T, RC4, QT, Embedded Web server and I2C

I. INTRODUCTION

A wireless sensor network (WSN) of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, LDR, Fire, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring The Internet of Things (IoT) refers to the interconnection of uniquely identifiable embedded computing-like devices within the existing

Sensor networks are expected to play an essential role in the upcoming age of pervasive computing. Due to their constraints in computation, memory, and power resources, their susceptibility to physical capture, and use of wireless communications, security is a challenge in these networks. The scale of deployments of wireless sensor networks require careful decisions and trade-offs among various security measures Since there is an increase in possible software attacks on privacy and safety of health applications, safety and reliability of the sensor data is an important issue that needs to be addressed in this field. A unique design of a secure sensor node prototype has been proposed and implemented.

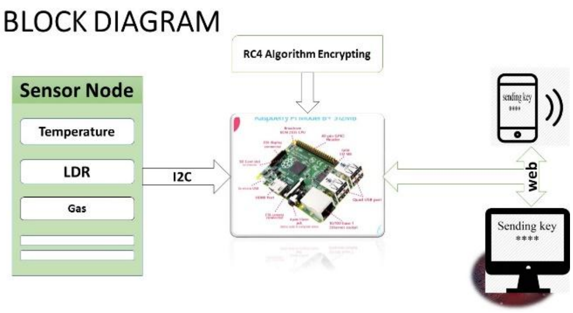
This prototype has sensor interfaces, where the data from the sensors are subjected to encryption and compression algorithms for future sensors. In this design, we using various sensors, like temperature and LDR sensor to implement the Security mechanism for the Sensor Node to avoid the possible software attacks and thereby eliminate the threats to safety, security and privacy of any industrial application system. Both safety and reliability of the sensor data is an important issue that needs to be addressed in these fields

II. PROPOSED SYSTEM ARCHITECTURE

Proposed architecture mainly consists of two modules. They are:

1. Secure sensor node
2. Server Module
3. Raspberry Pi

Sensor module consists of all the sensors which are used for data acquisition and sending these values to the server module through ZigBee, whereas the server module is the one which is responsible for receiving the values from sensor module and posting these values in the internet through server installed in it.



III. SOFTWARE SPECIFICATIONS AND FRAMEWORK

Software Specifications

1. Operating System : Linux
2. QT for Embedded Linux
3. RC4

1. Linux Operating System:

Linux or GNU/Linux is a free and open source software operating system for computers. The operating system is a collection of the basic instructions that tell the electronic parts of the computer what to do and how to work. Free and open source software (FOSS) means that everyone has the freedom to use it, see how it works, and changes it. There is a lot of software for Linux, and since Linux is free software it means that none of the software will put any license restrictions on users. This is one of the reasons why many people use Linux. A Linux based system is a modular Unix-like operating system

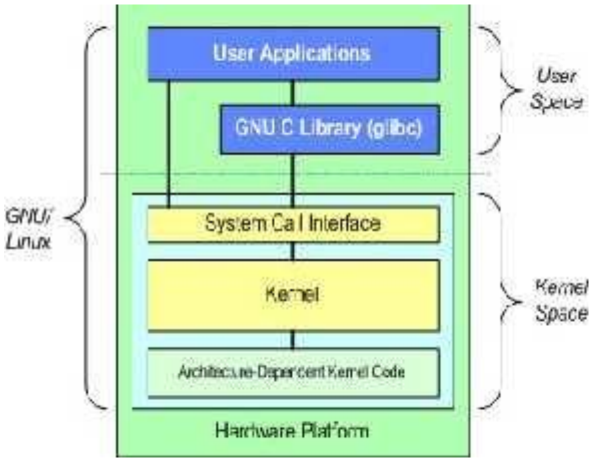


Figure.1: Linux OS Architecture

It derives much of its basic design from principles established in UNIX during the 1970s and 1980s. Such a system uses a monolithic kernel, the Linux kernel, which handles process control, networking, and peripheral and file system access. Device drivers are either integrated directly with the kernel or added as modules loaded while the system is running.

2. QT for Embedded Linux:

QT for Embedded Linux is a C++ framework for GUI and application development for embedded devices. It runs on a variety of processors, usually with Embedded Linux. QT for Embedded Linux provides the standard QT API for embedded devices with a lightweight window system.

3. RC4

RC4 is a stream cipher designed by Ronald L Rivest^2 for RSA Security. Ron Rivest is Professor of Computer Science at MIT's Department of Electrical Engineering and Computer Science. Ron is also the R in RSA. I mention Ron because RC is often referred to as “Ron’s Code” or “Rivest Cipher” and his home page has numerous articles explaining his various ciphers.

RSA holds the trademark for RC4 and commercial use is permitted only with a license from them. RC4 was released in 1987 and its internal workings are only disclosed by RSA with the purchase of a license. According to Wikipedia, the online encyclopaedia (MediaWiki), RC4 was anonymously leaked to the Internet Cypherpunks (Sterndark) mailing list in September 1994. Members of the Cypherpunks compared the “Alleged RC4” to RSA’s version and determined the results produced are compatible with each other. After the code was re-written it has been renamed to ARCFOUR to avoid trademark issues. Since I am not a legal expert, I will recommend you contact RSA for license information before using ARCFOUR in a commercial Application.

IV. HARDWARE IMPLEMENTATION SECURE SENSOR NODE

Sensor networks are a promising approach for a variety of applications, such as monitoring safety and security of buildings and spaces, measuring traffic flows, and tracking environmental pollutants. Sensor networks will play an essential role in the upcoming age of pervasive computing, as our personal mobile devices will interact with sensor networks in our environment.

Many sensor networks have mission-critical tasks, so it is clear that security needs to be taken into account at design time. Security will be important for most applications for the following reasons. Most sensor networks actively monitor their surroundings, and it is often easy to deduce information other than the data monitored. Such unwanted information leakage often results in privacy breaches of the people in the environment. Moreover, the wireless communication employed by sensor networks facilitates eavesdropping and packet injection by an adversary. The combination of these factors demands security for sensor networks to ensure operation safety, secrecy of sensitive data, and privacy for people in sensor environments .Security in sensor networks is complicated by the constrained capabilities of sensor node hardware and the properties of the deployment. Since sensor nodes usually have severely constrained computation, memory, and energy resources, asymmetric cryptography is often too expensive for many applications.

RASPBERRY PI BOARD

The **Raspberry Pi** is a credit-card-sized single board computer developed in the UK by the Raspberry Pi Foundation with the intention of promoting the teaching of basic computer science in schools. The Raspberry Pi is manufactured in two board configurations through licensed manufacturing deals with Newark element14 (Premier Farnell), RS Components and Egoman. These companies sell the Raspberry Pi online. Egoman produces a version for distribution solely in China and Taiwan, which can be distinguished from other Pi's by their red colouring and lack of FCC/CE marks. The hardware is the same across all manufacturers.

The Raspberry Pi has a Broadcom BCM2835 system on a chip (SoC), which includes an ARM1176JZF-S 700 MHz processor, Video Core IV GPU, and was originally shipped with 256 megabytes of RAM, later upgraded to 512 MB. It does not include a built-in hard disk or solid-state drive, but uses an SD card for booting and persistent storage.

The Foundation provides Debian and Arch Linux ARM distributions for download. Tools are available for Python as the main programming language, with support for BBC BASIC (via the RISC OS image or the Brandy Basic clone for Linux), C, Java and Perl.

The SoC used in the first generation Raspberry Pi is somewhat equivalent to the chip used in older smartphones (such as iPhone / 3G / 3GS).

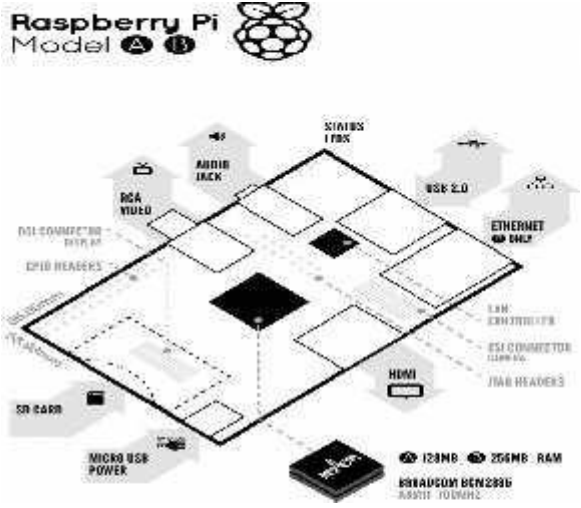


Figure 2. Board features

PCF8591T

The PCF8591 is a single-chip, single-supply low-power 8-bit CMOS data acquisition Device with four analog inputs, one analog output and a serial I2C-bus interface. Three address pins A0, A1 and A2 are used for programming the hardware address, allowing The use of up to eight devices connected to the I2C-bus without additional hardware. Address, control and data to and from the device are transferred serially via the two-line bidirectional I2C-bus.The functions of the device include analogy input multiplexing, on-chip track and hold function, 8-bit analog-to-digital conversion and an 8-bit digital-to-analog conversion. The maximum conversion rate is given by the maximum speed of the I2C-bus.

LIGHT DEPENDENT RESISTOR

Light dependent resistors are used to recharge a light during different changes in the light, or they are made to turn a light on during certain changes in lights. One of the most common uses for light dependent resistors is in traffic lights. The light dependent resistor controls a built in heater inside the traffic light, and causes it to recharge overnight so that the light never dies. Other common places to find light dependent resistors are in: infrared detectors, clocks and security alarms.

TEMPERATURE SENSOR (LM35)

The LM35 series are precision integrated-circuit temperature sensors, whose output voltage is linearly proportional to the Celsius (Centigrade) temperature. The LM35 thus has an advantage over linear temperature sensors calibrated in Kelvin, as the user is not required to subtract a large constant voltage from its output to obtain convenient centigrade scaling. The LM35 does not require any external calibration or trimming to provide typical accuracies of ±1/4°C at room temperature and ±3/4°Cover a full -55 to +150°C temperature range.

ETHERNET:

Ethernet LAN Features:

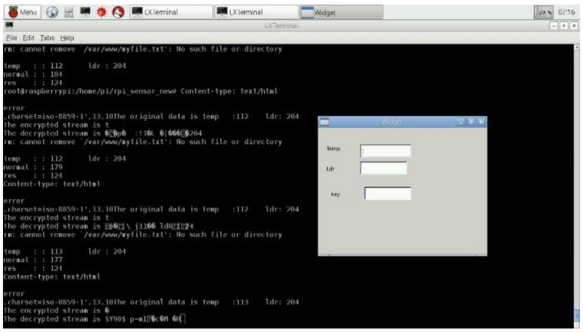
- Bus topology, Wired LAN in IEEE 802.3 physical layer standard
- 10 Mbps, 100 Mbps (Unshielded and Shielded wires) and 4 Gbps (in twisted pair Wiring mode)
- Broadcast medium─ Passive, Wired connections based.
- Frame format like the IEEE 802.2
- SNMP (Simple Network Management Protocol) Open system (therefore allows equipment of different specifications)
- Each one connected to a common communication channel in the network listens and if the channel is idle then transmits. If not idle, waits and tries again.
- Multi access is like in a Packet switched network

DISPLAY UNIT

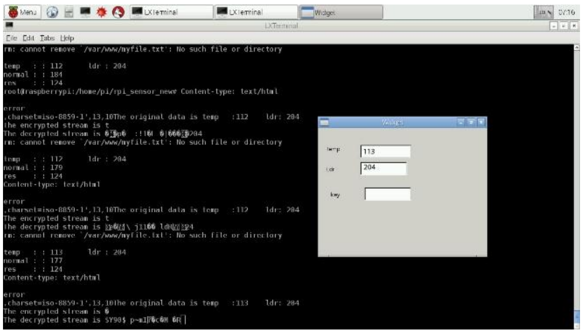
The encrypted data will be decrypted by RC4 algorithm by key sent by user by using HTML page from an embedded server that was installed in raspberry Pi both in desktop and mobile platforms the secure sensor data will be display on monitor with QT farmed environment

V. RESULTS

The project titled **"Raspberry Pi based RC4 encryption algorithm Implementation for Secure Sensor Node"** has been successfully designed and tested. It has been developed by integrating features of all the hardware components and software used. Presence of every module has been reasoned out and placed carefully thus contributing to the best working of the unit. Secondly, using highly advanced ARM11developwent board and with the help of growing technology the project has been successfully implemented.



```
rm: cannot remove `/var/www/myfile.txt': No such file or directory

temp   : : 112      ldr : 204
normal : : 184
res    : : 124
root@raspberrypi:/home/pi/rpi_sensor_new# Content-type: text/html

error
,charset=iso-8859-1',13,10The original data is temp   :112    ldr: 204
The encrypted stream is t
The decrypted stream is 6p6  :!16 6|666204
rm: cannot remove `/var/www/myfile.txt': No such file or directory

temp   : : 112      ldr : 204
normal : : 179
res    : : 124
Content-type: text/html

error
,charset=iso-8859-1',13,10The original data is temp   :112    ldr: 204
The encrypted stream is t
The decrypted stream is 6\ j1166 ldR24
rm: cannot remove `/var/www/myfile.txt': No such file or directory

temp   : : 113      ldr : 204
normal : : 177
res    : : 124
Content-type: text/html

error
,charset=iso-8859-1',13,10The original data is temp   :113    ldr: 204
The encrypted stream is 6
The decrypted stream is $Y90$ p-mI6c6M 6R
```



temp 113
ldr 204

```
rm: cannot remove `/var/www/myfile.txt': No such file or directory

temp   : : 112      ldr : 204
normal : : 184
res    : : 124
root@raspberrypi:/home/pi/rpi_sensor_new# Content-type: text/html

error
,charset=iso-8859-1',13,10The original data is temp   :112    ldr: 204
The encrypted stream is t
The decrypted stream is 6p6  :!16 6|666204
rm: cannot remove `/var/www/myfile.txt': No such file or directory

temp   : : 112      ldr : 204
normal : : 179
res    : : 124
Content-type: text/html

error
,charset=iso-8859-1',13,10The original data is temp   :112    ldr: 204
The encrypted stream is t
The decrypted stream is 6\ j1166 ldR24
rm: cannot remove `/var/www/myfile.txt': No such file or directory

temp   : : 113      ldr : 204
normal : : 177
res    : : 124
Content-type: text/html

error
,charset=iso-8859-1',13,10The original data is temp   :113    ldr: 204
The encrypted stream is 6
The decrypted stream is $Y90$ p-mI6c6M 6R
```

VI. CONCLUSION

According to a study conducted by The Telegraph, UK within the next decade, for the first time in human history there will be more people aged 65 years and older, than children under five in the world. A notable percentage of this population will reside in nursing homes and hospitals in times to come. In the future, these residences will employ pervasive networks which will provide continuous medical monitoring, control of home appliances, medical data access, and emergency communication. The body sensor module will be extremely beneficial to the patients and their caregivers who will be able to monitor their health on their own. It will enable doctors and physicians to remotely monitor their patients' health and improve the quality of healthcare, increasing safety

VII. FUTURE SCOPE

We plan to improve upon the design of the prototype by making it a battery operated with switches to start the sensor. The prototype can be used to implement other sensors and to investigate other encryption techniques along with new interfaces like Bluetooth low energy and NFC.

REFERENCES

[1] Texas Instruments, Inc., “OMAP4 Platform,” Technical report, Texas Instruments, http://www.ti.com/lit/ ml/swpt034b/ swpt034b.pdf, 2011.

[2] Qualcomm, Inc., “Snapdragon,” technical report Qualcomm,http://www.qualcomm.com/media/documents/snapdragons4-processors-system-chipsolutions-new-mobile-age, 2011.

[3] L. Sha, R. Rajkumar, and J. Lehoczky, “Priority Inheritance Protocols: An Approach to Real-Time Synchronization,” IEEE Trans. Computers, vol. 39, no. 9, pp. 1175-1185, Sept. 1990.

[4] J. Sang, C. Liang, C. Xu, and J. Cheng, “Robust movie character identification and the sensitivity analysis,” in Proc. ICME, 2011, pp. 1–6.

[5] T.P. Baker, “Stack-Based Resource Allocation Policy for Real-Time Process,” Proc. Real Time Systems Symp., 1990.

[6] P. Gai, L. Abeni, and G.Buttazzo,“Multiprocessor dsp Schedulingi n System-on-a-Chip Architecture,” Proc. Euromicro Conf. Real-Time Systems, 2002.

[7] K. Kim, D. Kim, and C. Park, “Real-Time Scheduling in Heterogeneous Dual-Core Architecture,” Proc. Conf. Parallel and Distributed Systems, 2006.

[8] S. Kato, K. Lakshmanan, R. Rajkumar, and Y. Ishikawa, “Timegraph: Gpu Scheduling for RealTime Multi-Tasking Environments,”Proc. USENIX Ann. Technical Conf., 2011.

[9] S. Kato, K. Lakshmanan, Y. Ishikawa, and R. Rajkumar, “Resource Sharing in gpu-Accelerated Window Systems,” Proc. Real-Time and Embedded Technology and Applications Symp., 2011.

[10] S. Saewong and R. Rajkumar, “Cooperative Scheduling of Multiple Resources,” Proc. Real-Time Systems Symp, 1999.