Middle-East Journal of Scientific Research 24 (9): 2816-2824, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.09.23871

Multi-Level Security of Embedded Systems in Internet of Things using Power Analysis

P. Muthu Subramanian and A. Rajeswari

Department of ECE, Coimbatore Institute of Technology, Coimbatore, India

Abstract: Internet of Things represents a major scenario in the history of the internet as connections move beyond computing devices and begin to power billions of everyday devices from intelligent traffic system to the missile navigation system. However IoT are prone to wide range of security concerns, except that of IP protocol constrains. Power analysis modules aid for an energy efficient electronic systems. But they can be inhibited in providing security by modifying them. Our objective is to develop a 3-layer security for IoT [(a) Online authentication (b) Data encryption (c) Power analysis model] and make the service provider active in the process. This approach can also be inhibited in securing the program codes in systems. Our objective is all based upon detecting the register files (RF) which are passive during the course of the program execution by register utilization. Initially a program-level granularity approach can be adopted by which the register level utilization of a set of benchmark codes can be visualized. Utilization of RF is more or less same for similar set of program codes can be used. For instance, all the basic math or string-search or quick-sort consumes RFs of close numbers of their same kind with respect to the number of instructions. This property is used for unique identification of similar set of codes in the embedded systems. In case of any intruding foreign codes there occurs an abnormality in the perspective of power related to the one with respect to that of the usual set of codes.

Key words: Embedded Systems · Microcontrollers · Power Analysis · Security

INTRODUCTION

This section deals with the necessity of the paper and the background and motivation behind it. The world around us is getting smarter and autonomous in remarkable increase in growth. It is important for the service providers to increase the level of security provided to any embedded computing applications devices. The latest wave of connectivity is "things" connecting to users, businesses and other "things" using mixtures of wired and wireless connectivity. This includes automobiles, airplanes, medical machinery, personal medical devices, windmills, environmental sensors and any embedded computing applications devices. The effectiveness and efficiency of these systems is being greatly multiplied by both client/server and peer to peer connectivity, enabled by advances in new forms of connectivity inexpensive controllers and Internet-standard protocols. The effectiveness and the efficiency of the systems are increased in a numerous way but we lack in providing the appropriate security to the “things” and as a result the system can be hacked and used by unauthorized pirates [1]. Critical Security Controls will be needed in the Internet of Things. The way security is architected, delivered and monitored will need a change. The main objective of the project is to create a multilayer IoT security where the corresponding security layers are online authentication which includes a authenticate code which gives access connection between the user and the server then followed by second layer, data encryption and as the third layer power analysis model is undergone and the adopted power analysis model based on detecting the register files (RF) which are passive during the course of the program execution by register utilization. In a model of Reducing Register File Static Power unused registers for specific set of instructions were found and power gating method is followed to make the registers unavailable in order to reduce the power consumption. In measurement of current variations for the estimation of software related power consumption, the current consumed for each instruction cycle is calculated using current mirror and with the help of software [2]. The existing technologies

Corresponding Author: P. Muthu Subramanian, Department of ECE, Coimbatore Institute of Technology, Coimbatore, India.

are very time-consuming and impractical techniques for the evaluation of the power consumption of embedded software [3]. Moreover, they cannot even be applied in most cases, due to the lack of availability of circuit and gate level information of the embedded processors.

Survey: There are number of techniques as a result of the development of security layer for embedded systems, designed according to some new concepts established in this field during the last decade. Among those, Internet connected things that touch very sensitive personal information are high priority targets for cyber criminals. In both of these areas, new technology requiring new approaches to security will be added to legacy systems employing legacy security processes and technology while the same Critical Security Controls will be needed in the Internet of Things, the way security is architected, delivered and monitored [4]. The security we are targeting is mainly on the field of analyzing the power consumed in embedded computing application devices. Power and energy consumption are on the top priority list in embedded computing [5]. Embedded processors taped out in deep submicron technology have a high contribution of static power to overall power consumption. At the same time, current embedded processors often include a large register file (RF) to increase performance [6]. However, a larger RF aggravates the static power issues associated with technology shrinking. Therefore, approaches to improve static power consumption of large RFs are in high demand.

Unused registers for specific set of instructions were found and also Power gating method is followed to make the registers unavailable in order to reduce the power consumption. But apart from reducing the power consumed our project objective is to determine the contribution of power that is consumed for each and every instruction. At present, power measurement tools focus mainly on the lower levels of the design; at the circuits level, at the logic level and to a limited extend at the RT level [7]. Generally, these are very time-consuming and impractical techniques for the evaluation of the power consumption of embedded software. Moreover, they cannot even be applied in most cases, due to the lack of availability of circuit and gate level information of the embedded processors. The embedded processors currently used in designs are of two kinds: ‘off-the-shelf’ microprocessors and the embedded cores. In the first case, the information available is usually included in the data books, while in the second case, the designer has logic/timing simulation models as a design verification [8].

In neither case the lower level information is available for the power analysis of the software. There are many advantages in developing an instruction-level power consumption model for a processor [9]:

- Estimation of the power cost to the software component of a system
- Verification of overall system's power budget
- Useful information for high-level design decisions such as hardware software partitioning
- Development of automated code generation tools with low power features, etc.

Each instruction involves specific processing activities across various units of the processor. These processing activities are performed by associated circuit activities which are characteristic for each instruction and therefore vary with different instructions.

Service Provider Unit: The proposed model is providing three levels of security to prevent the intrusion of foreign intruders and the three levels are achieved by obtaining OTP and followed by that username and password verification and as the final level of providing security is achieved by power analysis of the target processor or machine. The overall flow of the proposed system in shown in Fig. 3.

Fig. 3.2 represents the overall flow of the proposed system where the service providers are mentored to establish the interconnection between the user interface and the target system by online authentication.

User: In order to prevent the software theft, we are providing the platform and thus allowing the user to have control of their target machine through internet irrespective of their current location. Each authenticated user should have their corresponding unique identification code and password. By using this id and password the user can control the target machine anywhere from the world. By using this we can prevent the unauthorized users.

Target Machine: Target machine may be the embedded processors or any hardware instruments that the user wants to access. Here we process processor as a target machine. Once the target machine is doing a process the amount of power consumed is calculated and it is stored in database.

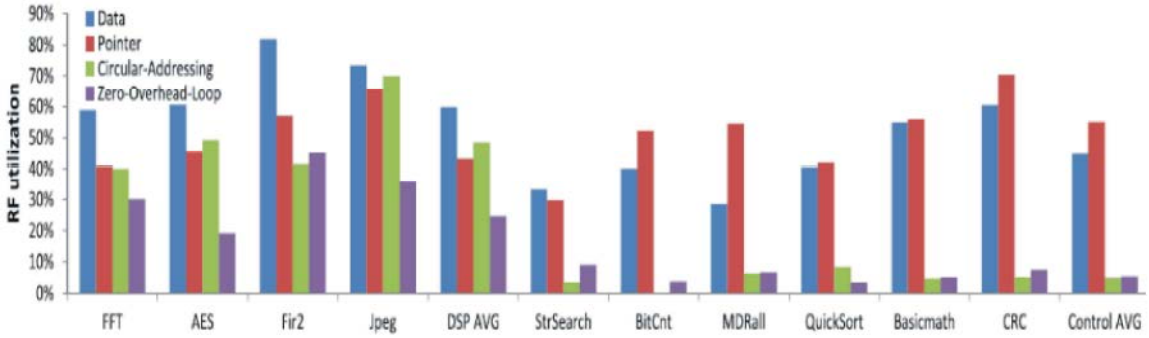


Fig. 1: The Register Comparison

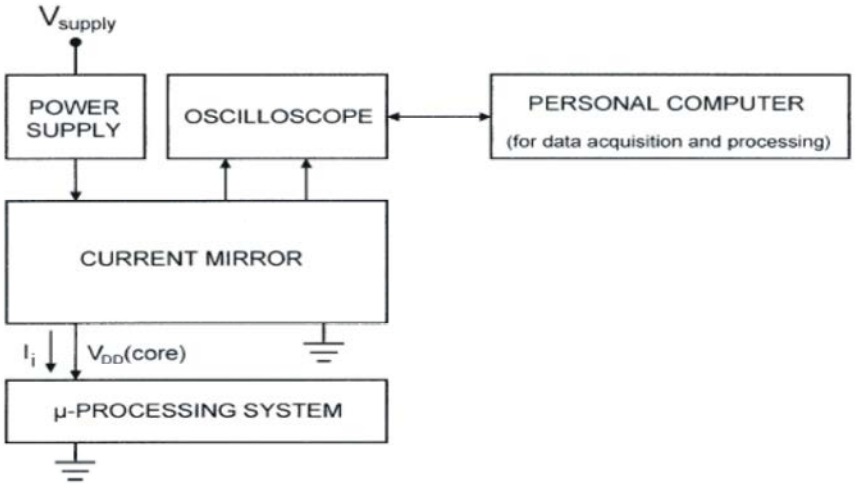


Fig. 2: Block diagram for current level measurement

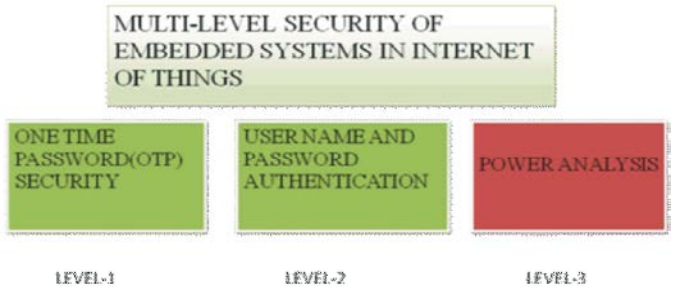


Fig. 3: Proposed System (Three Levels of Security)

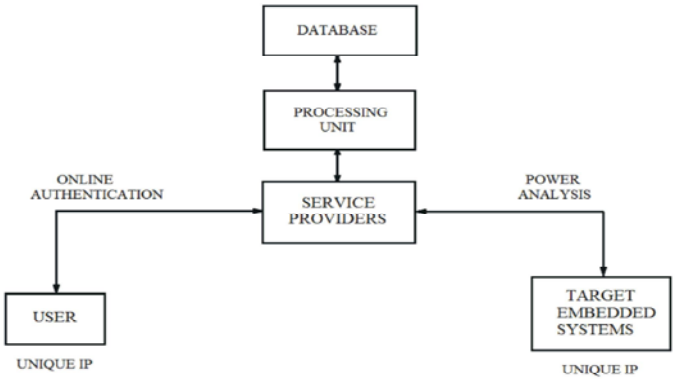


Fig. 3.2: Block diagram of the proposed system

Database: A separate database is created to maintain the account of each user. In the database we are having the records of user name, id, password, date and time of login and power consumption of the target machine for every login. Thus by having the whole record we can able to know complete details of all users and their activity.

Service Providers: Service providers act as a bridge between the user and target machine. They also provide the second level of security by creating OTP from the data available from the database. The generated OTP is notified to the users through mail or by message. During login time they should enter their unique OTP created during that entry which improves the level of security. Third level of security is provided by the service providers by comparing the power consumed by the target machine with the previously consumed power level or from the threshold power level available from the database. If the power level testing is not satisfied the service providers will automatically turn off the target machine and it alerts the admin that there is an illegal entry.

Username Authentication: This comprises of the conventional username and password security which has been obtained from the device user at the time of account creation. This provides a very fundamental security for the internet of things which are prone to illegal access by intruders. The user encounters with the authentication by providing their username and password in the login page as shown in the Fig. 4.1.

The fundamental user information's like username, email id, phone number, password to validate a user are received at the first instance of a new user. These users information's are stored in the server database which are managed by SQL and. It is structured by the aide of ASP.net using C Sharp and cascade style sheet (CSS) for its controls and front end design. Whenever the user tries to log into the system the basic information of the user like id, password, e-mail address, date and time in which the user logged into the system are stored in the database using SQL. This is illustrated in the Fig. 4.2. security. Third level of security is provided by the service providers by comparing the power consumed by the target machine with the previously consumed power level or from the threshold power level available from the database. If the power level testing is not satisfied means the service providers will automatically turns off the target machine and it alerts the admin that there is an illegal entry.

Username Authentication: This comprises of the conventional username and password security which has been obtained from the device user at the time of account creation. This provides a very fundamental security for the internet of things which are prone to illegal access by intruders. The user encounters with the authentication by providing their username and password in the login page as shown in the Fig. 4.1.

OTP Generation: In order to provide higher grade of security, we go for the one time password (OTP). This can be flexed and implemented as per the user's need and convenience. The generation of this password is based upon the MD5 (Message Digest-5) algorithm, which is one among the data encryption algorithm usually used at instances like 'forgot password' [9]. Visual studio is used to interface the HTML front end and the database from the SQL. It bridges the user with his individual information which is already obtained. Moreover, visual studio has the privilege that it can generate the OTP using the MD5 algorithm which is available as input function, every time the user attempts to establish a connection with his own end thing or device the generated OTP can either be sent to the user via short message service (SMS) or Electronic Mail Services. The operation of MD5 algorithm is as follows:

MD -5 ALGORITHMS

Example:
Hexa decimal value for 5: 0000 0101
0000 0101 0000 0000
0000 1010 0000 1010
0001 0100 * 0001 0100

0010 1000 0010 1000
…. ….
…. ….

== [MATRIX]

Matrix is formed by left shifting the digits, till the last digit comes to the first. The obtained square matrix and its inverse is multiplied to get the resultant matrix. From resultant matrix Eigen values and equivalent hexadecimal values are calculated. From the hexadecimal value we can get the OTP [ONE TIME PASSWORD]. Thus service provider creates the OTP for each entry and displays that to the user through message or e-mail as represented in Fig. 4.3.

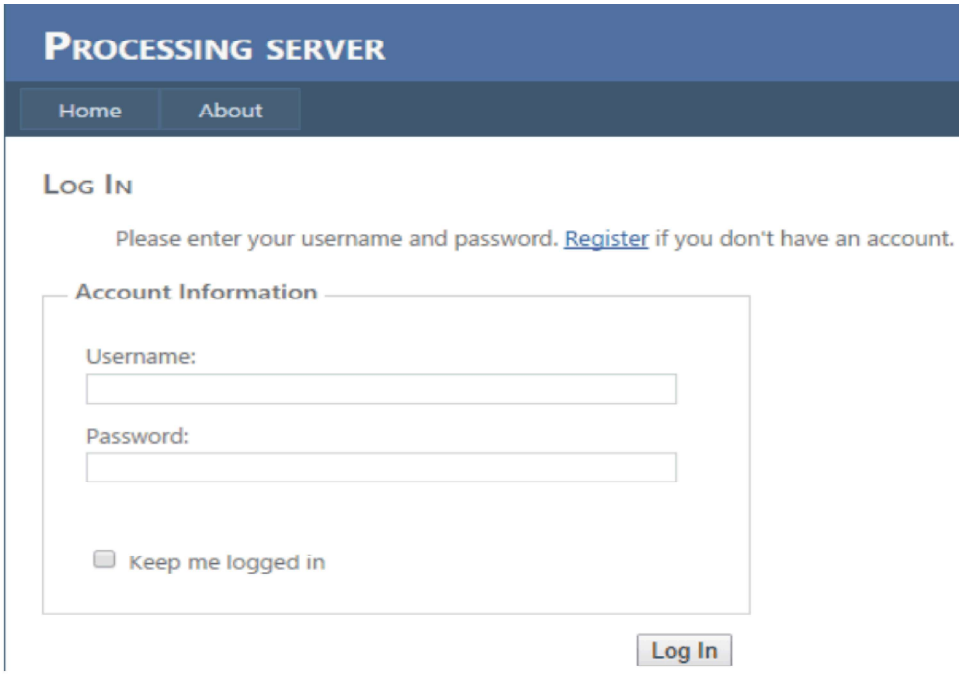


Fig. 4.1: Home page

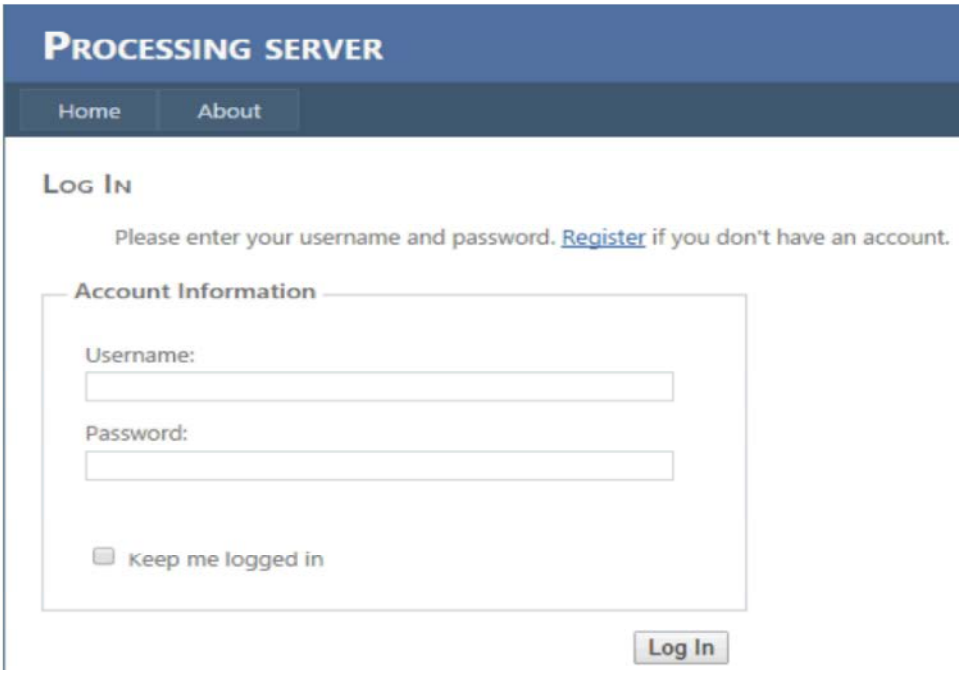
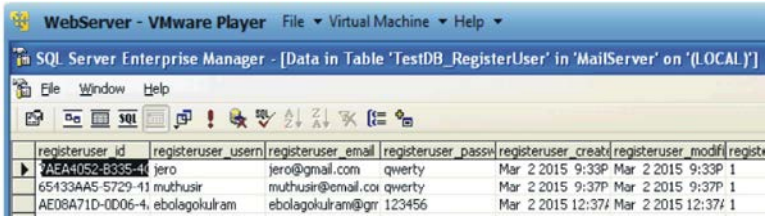


Fig. 4.2: Home page



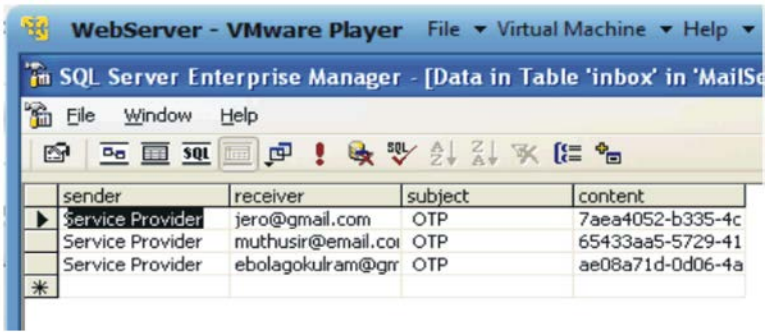


Fig. 4.3: Displaying OTP

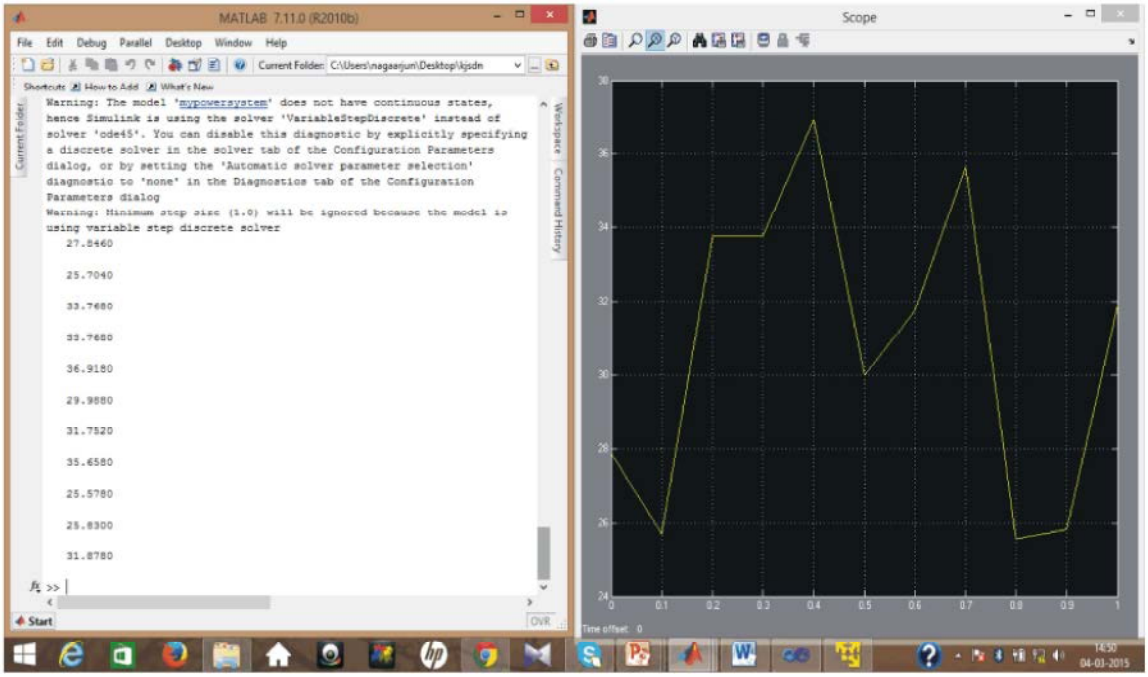


Fig. 4.4: Power consumption in Matlab

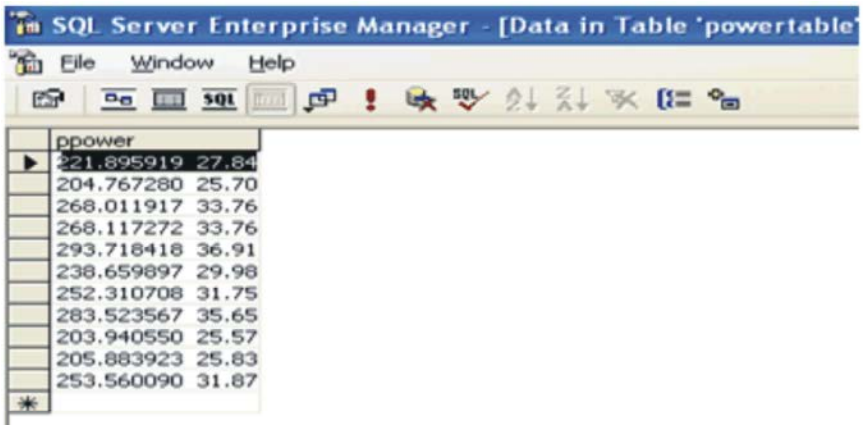


Fig. 4.5: Power consumption in Server

Following algorithms like Security Hash algorithm (SHA-1), Elliptical Curve Digital Signature algorithm (ECDSA), RSA can also be used to generate One Time Password. In order to interface the ASP.net and MySQL, Visual studio is used. It provides code behind them to manipulate the event of control.

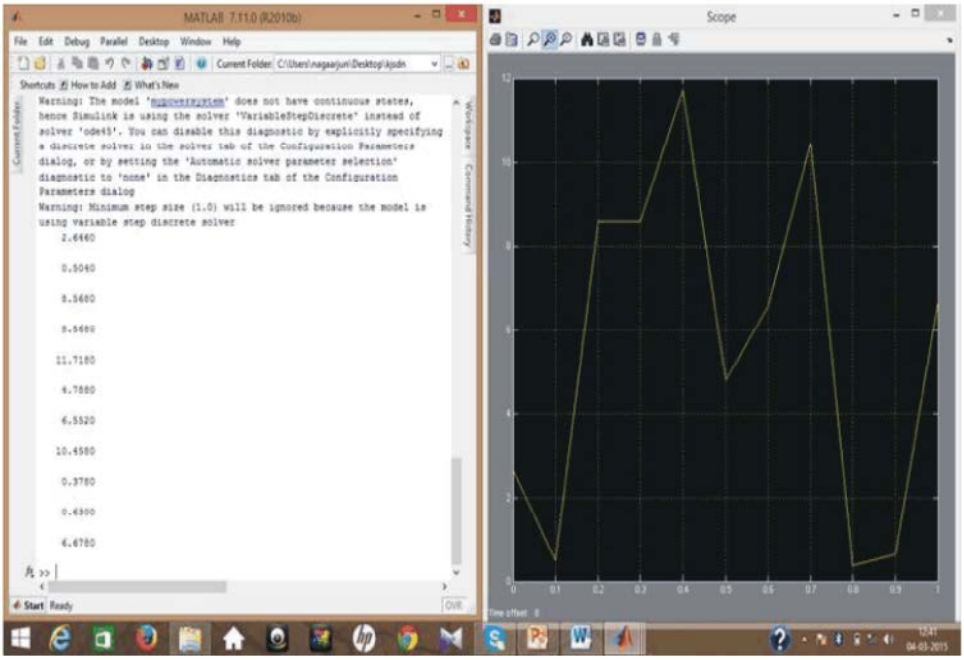


Fig. 4.6: (0-100 RANDOM NUMBERS)

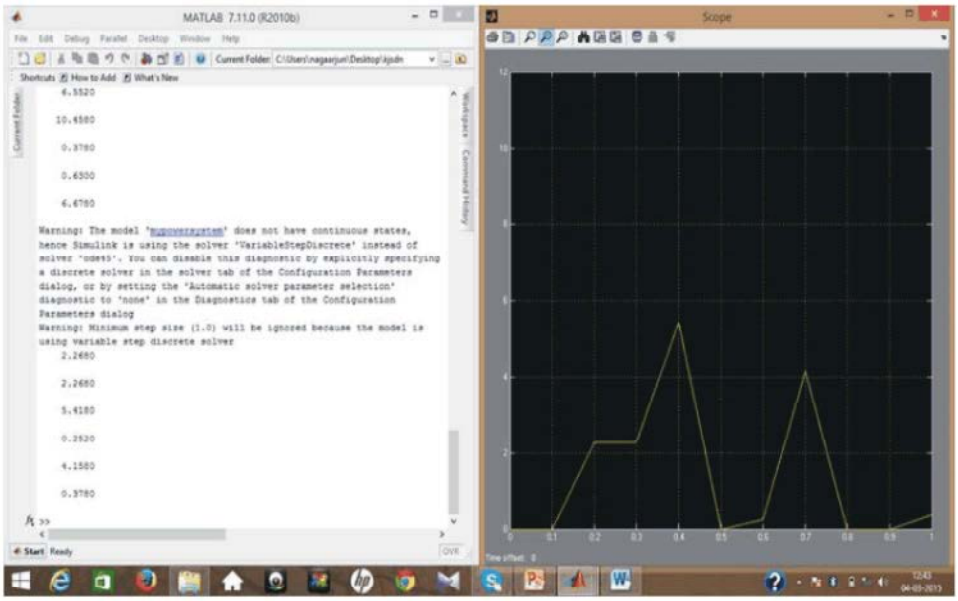


Fig. 4.7: (200 to 300 RANDOM NUMBERS)

Power Analysis: The third layer of security is provided by analyzing the power consumed by overall process and also by the each instruction level. Software constitutes nowadays a major part of systems like embedded computing applications drives where power is a constraint and also has a significant contribution to the overall power consumption [5]. In order to analyze systematically and assess this impact, it is important to start at the most practical and fundamental level –the instruction level. The instruction level power models are derived based on the power supply current measurement technique. Each instruction took a specific amount of machine cycles to complete its operation. The number of machine cycles varies from one instruction to another. From which time taken for each instruction set to execute is calculated and by using that overall time elapsed was found. With the help of time elapsed and operating frequency we can able to calculate power consumption.

Power consumption for each process is calculated periodically as shown in the Fig. 4.4 and it is updated periodically in the database as represented in the Fig. 4.5 with the help of visual studio and SQL. The threshold value is obtained from the series of power values available in the database. Target machine's power consumption is compared with the threshold level and if the power ratings does not match service provider will turn off the host.Power variations are based on:

Changes in Complexity of Program: As the complexity of instruction set for different operations increases, it is an evident increase in the overall power consumed by the process.

Changes in the User-Given Data (Random Number): As the random number changes there is change in the number of iterations of the processes which in turn changes the power obtained. Let us consider the case, that in the Fig. 4.6 and 4.7 both performs the same operation but the input given to the operation varies. The change in input reflects directly on the output as it changes the power consumption of the process.

RESULTS AND DISCUSSION

Registration: Login page shown in the Fig. 4.1 is available to the user to enter into the system and controls the access of the target machines. If the user does not have an account, they can create their new account by clicking the REGISTER icon available on the page as shown in the Fig. 6.1 by providing mail address, password, and confirmation password. In this a user can create their account in the server.

Authentication: Once the user creates the account, information's regarding the user is stored in the database. With the help of available information's authentication takes place. During login time user should enter their id and password. If the entered data matches with the existing data available in database user can allowed to login to the systems otherwise an error message will be displayed as 'invalid username or password' as shown in the Figure. 6.2.

OTP: Second level of security is obtained by creating One Time Password. One Time Password is created with the help of Message Digest - 5 algorithm using username and password. OTP is sent back to the user through email as mentioned in the figure 6.3. During the time of login user has to enter the OTP which improves the level of security.

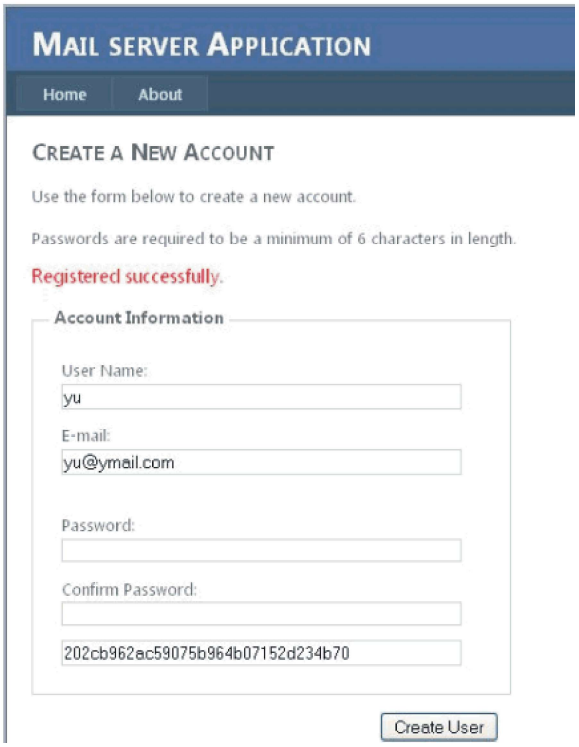


Fig. 6.1: Registration

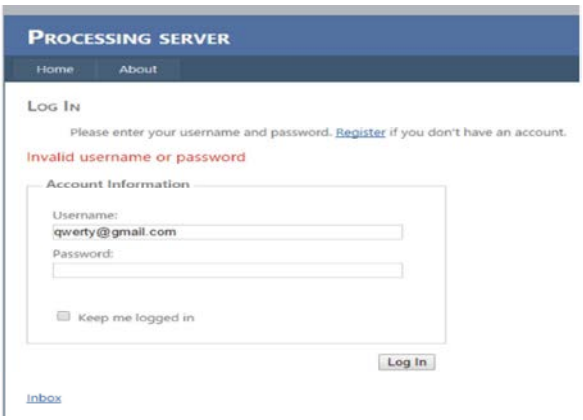


Fig. 6.2: Error Message

Fig. 6.3: OTP Verification

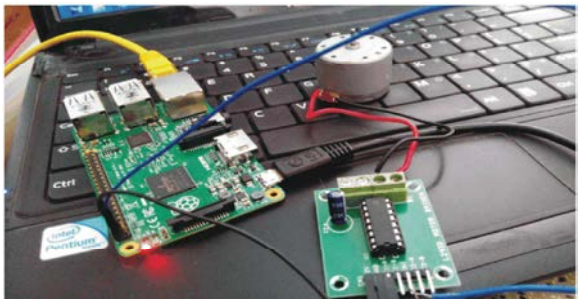


Fig. 6.4: Raspberry kit with target device

Fig. 6.5: Controlling the target device using IoT

Power Analysis: The power is analyzed for each process and calculated periodically for the raspberry pi kit with target device as shown in the Fig. 6.4 and it is updated periodically in the database and the target device works for the normal set of operations as represented in the Fig. 6.5

CONCLUSION

The software implementation can be developed; simulated and verified using the Xilinx tool and the program coding for username authentication and generation of OTP is generated and maintained using MySQL, HTML and CSS. The power is analyzed using the power report generated in the Xilinx tool. Future work is to additionally improve the hardware security like finger print, palm match, retinal scan, and gesture and RFID techniques. Additionally PC's and mainframe computers-compatible for hardware interfacing only, Smartphone's and tablets-tedious to be provided with hardware security and reduction in hardware complexity to provide security and supports virtual security.

REFERENCES

1. Borja Martinez, Marius Monton, 2015. "The Power of Models: Modeling Power Consumption for IoT Devices", IEEE Sensor Journal, 15: 5777-5789.
2. Ranjithkumar, 2008. "Technique for accurate power and energy measurement with the computer-aided design tools" IEEE, 17(3): 399-421.
3. Hamed, Tabkhi and Gunar Schirner, 2013. "Application- Guided Power Gating., Reducing Register File Static Power" IEEE, 63: 8206-8210.
4. Qian Xu, Pinyi Ren and Houbing Song, 2016. "Security Enhancement for IoT Communications Exposed to Eavesdroppers with Uncertain Locations", IEEE Access, 4: 2840-2853.
5. Hawit, T., 2015. "Measurement of current variations for the estimation of software related power consumption" IEEE, 53: 7280-7285.
6. Theodore Laopoulos, Periklis Neofotistos, C.A. Kosmatopoulos and Spiridon Nikolaidis, 2003. "Measurement of Current Variations for the Estimation of Software-Related Power Consumption" IEEEVOL, 52(4).
7. Novak, M., J. Novak, M. Cambál and I. Uhlír, 2008. "Digital measurement of power in impulse powered circuits" 8th International Scientific - Technical Conference Process Control, 2008. June 9 – 12.
8. Vivek Tiwari, 2011. "Software Power Estimation and Optimization.", IEEE, 13(2): 1065-1069.
9. Sachin Babar, Neeli Prasath and Ramjee Prasad, 2011. "Proposed Embedded Security Framework for Internet of Things (IoT)" IEEE, 978-1-4577-0787.