DESIGN OF WI-FI INTEGRATED SOPHISTICATED METER USING EMBEDDED SYSTEM

Iswarya.V
PG Scholar, K.S.R. College of Engineering/ECE, Tiruchengode,India

ABSTRACT: **Focusing on a recent real time issue Electricity Hacking and malactivities in bill processing, a prototype Impregnable Device for secured metering (IDSM) is designed which consists of a sophisticated meter(SM) differing from other meters in security with a legacy Wi-Fi system for communication, a microcontroller, a centralized monitoring and control unit implemented cost effectively and a C Database Management System for data backing. In order to provide security at a higher level various cryptography techniques are to be analyzed and the most secure cryptography Random number Address Cryptography (RAC) is chosen. For wireless communication to be more efficient Radio Frequency (RF) is used designing a wide range to cover longer distances. The SM present in each house is connected by wireless network which periodically gets updates from the server. The server using a backend database calculates the amount to be paid according to the number of units consumed and sends it back to the meter for display at home along with the required information which reduces manpower along with the grievances. Our prototype focuses on security, communication at a higher speed with an advanced metering and a unique database for backend system.**

Index Terms:- **Cryptography, Sophisticated meter, legacy Wi-Fi, CDBMS, unconditional security.**

I. INTRODUCTION

Embedded systems are widespread in consumer, industrial, commercial and military applications. Networking in embedded systems is needed to integrate devices for any application so they are increasingly widespread and important. Many real time applications nowadays are dependent on integration of many systems which allow efficient, ubiquitous computing, intelligent system, cost effective implementation, efficient power utilization concerning memory etc.. In many situations a communication link between two devices becomes essential. This communication can be wired or wireless. Radio Frequency (RF) communication has a wide range, from few meters to millions of kilometers, does not require two devices to be in line of sight, can cross many obstacles. When communication is wireless hackers are more than in wired communication. Security plays a vital role in all applications, there are many reasons to protect the information used on the computer and during communication. Considering a recent real time issue, let us consider electricity hacking along with the electricity billing system in existence, for this we take an example of this trend the metering infrastructure that can be used in both domestic and commercial purposes.

Our prototype IDSM deals with a specially designed architecture on whole comprising of a client module and a server module.

The client module comprises of electrical devices in domestic or commercial purpose whose power consumption is calculated using a SM differing from other meters, an Atmel 89C51 microcontroller to receive the data from the meter and communicate with other devices via legacy Wi-Fi and a legacy Wi-Fi transceiver unit specifically designed for communication between the client and the server.

The Server module comprises of a legacy Wi-Fi transceiver unit which communicates with the client, a data acquisition unit for receiving the data from legacy Wi-Fi and transferring it to the centralized monitoring and control unit, a centralized monitoring and control unit monitors and controls the whole architecture. It is generally a desktop or an individual system and a CDBMS which is a database that generally backs up the data.

II. REVIEW

Application oriented project – Advanced Metering Infrastructure.An architecture for providing remote attestation for advanced meters, called a *Cumulative Attestation Kernel (CAK),* is implemented at a low level in the meter and Cryptographically secure audit data.Data integrity on meters can be compromised by malicious application firmware in various ways. Three modes of attack on sensor data available to malicious application firmware running during various lifetime phases occupied by that data. Data acquisition is not reliable, stored data may be corrupted or deleted leading to data corruption or misled. Application is remote so attackers are more. Elliptic curve Cryptography is used for security. Attestation is either from a mobile or a desktop in which response time is short so in any process delay in response affects the whole system. Cost of Implementation is high[1]. Universal connectivity of embedded system provides increased possibilities for malicious users to gain unauthorized access to sensitive information. Various attacks at different abstraction levels are defined. Security is needed at both data transfer and within the device[3].Smart home device descriptions and standard practices for demand response and load management "Smart Energy " applications needed in a smart energy based residential or light commercial environment. Alogrithm used is Disjoint Multi Path Routing protocol, Kruskal's algorithm, Sensor Network Analyzer(T)[6].Wireless LAN-IEEE are licence free bands available worldwide.Security is less as no authentication is provided.Two requirements are highly considered, QOS in real time environment over non-real time and power saving that meets user's perspective.bEDCA + S-APSD(Enhanced distributed channel association, Scheduled Advanced power save delivery) is best suited for bidirectional applications with no periods of no activity [7]. System uses wireless communications from consumer home to EB office with the help of GSM using a RFID in both ways. Reduced manual labour, taking time, power Blackout. Along with a billing information via SMS sent . RF signaling and Ad-Hoc data transfer can be used in various fields[8].Single chip VLSI processor–HCgorilla needs more complicated strategy, involves parallelizing compilers . The prototyping compliers are written in Java. Compilation Techniques are Multicore compiler, LIW compiler[9].The following proposed methods are analysed key-based multiple Huffman tables(MHT), arithmetic coding with key-based interval splitting(KSAC) and randomized arithmetic coding(RAC).Our analysis shows that MHT and KSAC are vulnerable to low complexity known and /or chosen plaintext attacks. Although we do not provide any attacks on RAC , we point out some disadvantages of RAC over the classical compress then encrypt approach. Other approaches under argument do not have advantages over RAC in terms of efficiency and security[10]. Secure architecture based on virtual machines and attestation for software agents that use meter.TPM and Xen VMM are used in prototype. First approach using virtual machine. ESP isolution is made less vulnerable to a variety of security threats. Advance metering systems may be connected to the Internet or even a wireless network that is highly vulnerable to eavesdropping and physical attacks.IA32 architecture based on embedded processors such as ARM.Due to space restrictions many issues surrounding software distribution, updates and removal are not addressed[11]. Ubiquitous system has dual features diversity and threat.RAC is developed in a single chip unique processor to run on any platform. Found effective as it considers whole text without division and does not involve any arithmetic operations, performed using simple memory access. Memory scrambling is done at hardware along with software support. A dedicated processor is needed to achieve sufficient speed, performance and strength used for low power and high throughput[12].Anecdotes obtained from an installation on a large industrial power system. IED configuration with PLC. Integrates many functions with minimal maintenance/testing, uploading and downloading of data and logs in serial communications [13]. Government: In order to reduce electricity theft and to calculate power consumed govt has introduced a new technique in which ESP client notifies the reading from the street instead of notifying each house.A LPRF receiver captures the transmitted data from the houses,for that a repeater is placed along with ordinary meter and immediately registers data online.The work done by the government was not yet transparent, and the real technology behind that is not yet revealed. All the present data was just an overview, and got with the help of bing.com

III. NEED AND APPROACH

A. Need for Security:

The universal connectivity for embedded systems creates increased possibilities for malicious users to gain unauthorized access to sensitive information. The security of today's systems is appallingly bad. Attacks on these systems are getting sophisticated. Malicious data can be sent to unsecured back-end databases and other systems that are susceptible to common attacks. In networked embedded systems an attacker does not need to physically possess the system. Embedded system security often requires protecting critical or sensitive information (code or data) throughout its lifetime. Potential attacks first must be identified which can come from both internal and external sources. The security needs for an embedded device thus can be classified into two, Security needs for data transfer and Security needs within the device. So it is desirable that information stored in a system is free from unauthorized alteration throughout its lifetime and it is properly erased at the end of its lifetime. Security should be taken into account during the design phase .Proper security solutions should be found for Message authentication, Key management, Encryption. Access to the embedded networks should be restricted to authorized users. Security functions implemented in an embedded system must be considered in both hardware and software.Security defined in a system is to identify threat, set targets, assess risks, device countermeasures (people, processes, measures and procedures).

B. Secure Measures:

The common security objectives which need to be satisfied by security protocols are confidentiality, integrity, authentication, non-repudiation and availability. Cryptography is the technique for secure communication in the presence of third parties, not only protects data from theft or alteration, but can also be used for user authentication. On analyzing the commonly used cryptography techniques that are generally used we infer that the most commonly used cryptography technique is Elliptic Curve Cryptography (ECC) followed by Ron Rivest, Adi Shamir and Leonard Adleman(RSA)., in competency with other algorithms.

ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements.

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Whether breaking RSA encryption is as hard as factoring is an open question known as the RSA problem.

So Random Number Addressing Cryptography (RAC) is considered.RAC is a common key technique with ideal cipher strength like vernam cipher in which the plaintext is combined with the "key stream" of the same length, to generate the cipher text, using the Boolean "exclusive or". RAC is theoretically high speed, because it does not do any arithmetic logic operation speed and simple like XOR, but does simply memory access. Due to its high memory access without any arithmetic logic operation, RAC shows its merit to achieve usability and safety. Memory scrambling is done at hardware along with software support. A dedicated processor is needed to achieve sufficient speed, performance and strength used for low power and high throughput.

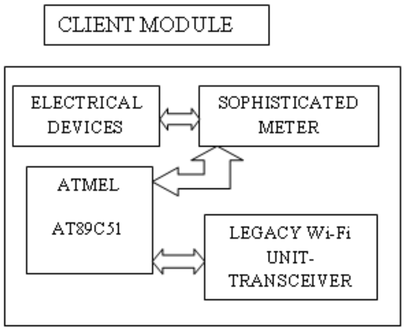
It owes a multicore architecture to enhance throughput with less power. The power conscious highly performance of RAC is due to a novel architecture following symmetric multicore, superscalar, and LIW (Long Instruction Word) processor techniques. LIW is not so broad parallelism like VLIW (Very Long Instruction Word), yet it is effective to practically enhance multimedia communication that deals with large quantity of data in pervasive environment. A Ubiquitous system has dual features diversity and threat. Since, it is expected that the input data is longer than the compressed data, the RAC efficiency is expected to be worse than that of the standard approach. Provably secure schemes are more appreciated than heuristic scheme. The standard approach is proven secure assuming that the PRBG is cryptographically secure. If one can break the encryption scheme, then one can distinguish the output of the PRBG from a random sequence. So far, such proof has not been provided for RAC.

C. Other parameters:

Embedded systems have special limitations concerning cost, power efficiency, computation, and memory that influence how this goal can be achieved. The power efficiency when compared with other computation of various techniques in cryptography state that RAC consumes less power when compared with other cryptography, on considering cost the prototype to be implemented in the project is cost efficient.

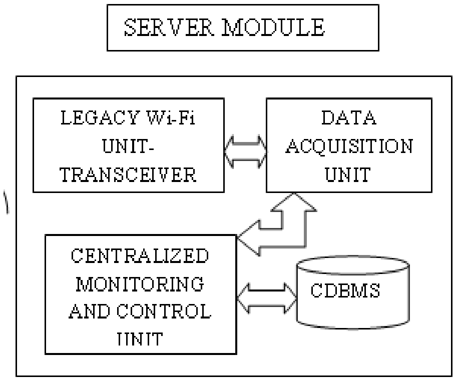
IV. SYSTEM MODEL:

A. CLIENT MODULE:



The client module refers to the HAN home area network which considered domestic may also be applied in commercial purposes. It comprises of certain units which are Electrical devices refer to the appliances in common that consume power to function and the power consumed is analyzed using a Watt-Hour meter. The Watt hour meter is designed with additional features and referred as a sophisticated meter. The AT89C51 is a 8-bit microcomputer with 4Kbytes of Flash Erasable and Programmable Read Only Memory (EPROM). The Atmel AT89C51 is a powerful microcomputer which provides a highly-flexible and cost-effective solution to many embedded control applications In many situations a communication link between to devices becomes essential for that RF communication is used. A frequency is defined for transmission and reception between the devices, it covers a Wide range, from few meters to millions of kilometers it does not require the two devices to be in line of sight and can cross many obstacles.

B. SERVER MODULE:

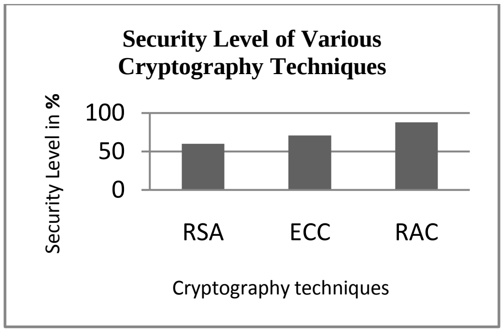

SERVER MODULE
LEGACY Wi-Fi UNIT-TRANSCEIVER
DATA ACQUISITION UNIT
CENTRALIZED MONITORING AND CONTROL UNIT
CDBMS

The server refers to the EB office which collects the information from the client modules via connectors (if necessary) which are domestic may also be applied in commercial purposes. Data acquisition unit is a system that acquires the analog data and converts it into digital data. It allows you to measure currents, voltage, and temperature, etc... Simple modules can be used for personal, small lab projects. Industrial uses include testing of battery, fuel cell, etc...Here atmel89C51 is used as a data acquisition unit. The centralized monitoring and control unit that is generally used here is a simple desktop system and it does not require any server connected with many client systems. The data will be stored in CDBMS a data base system for 'C' Database Management System.

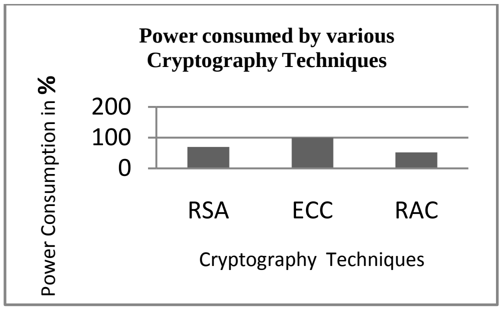
V. CONCLUSION

A. Analysis

The various cryptography techniques have been analyzed for various inputs such as text, image,etc using hackman tool and the tool on analysis reports that RAC is found more secure than other cryptography techniques in existence.



When considering in a networked embedded system power and memory are also factors that are considered in equivalent to security as power affects computation speed, computation time etc. Memory utilization must also be considered during implementation.

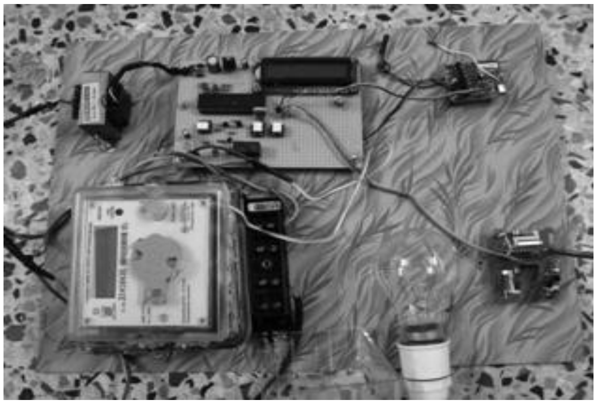


B. Communication Medium

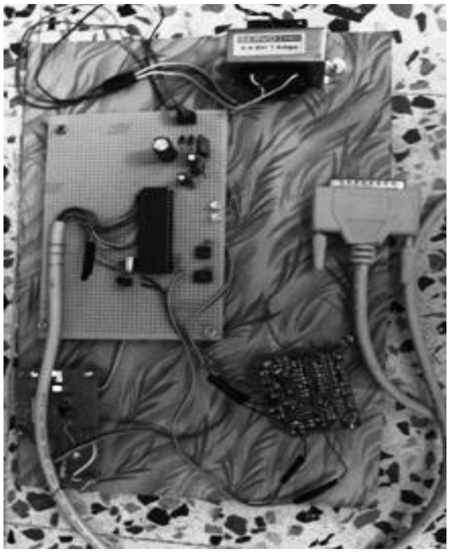
While considering the wireless standards that are available for communication, the IEEE standards are license free bands and are easily vulnerable. So attackers and possibility of data theft is high. RF is used in this project where a frequency is defined for communication which can communicate longer distances effectively.

C. IDSM

Our prototype on whole comprises of SM is a specially designed Watt-Hour meter which comprises of the single phase Watt-Hour meter integrated with an LCD display and a microcontroller. It furnishes the data acquired in a secure way using cryptography techniques. The ways for hacking data remains easier during communication. It overcomes factors such as response time, cost of implementation and security at a higher level when compared with the available techniques. A legacy Wi-Fi unit is designed using RF communication to cover a wider area and a multimedia encryption technique is to be made easier for secure data transaction and a demo of the prototype is done which can be applied in higher to provide a better system than in existence



Prototype - Client Module



Prototype - Server Module

REFERENCES:

1. Michael LeMay and carl A. Gunter, Senior Member,[2012] ”Cumulative Attestation Kernels for Embedded Systems”, IEEE Transactions on Smart grid, vol. 3, no. 2,pp.744 – 760,
2. Francesco Benzi, Norma Anglani, , Ezio Bassi, and Lucia Frosini [2011] ” Electricity Smart Meters Interfacing the Households”, IEEE Transactions On Industrial Electronics, vol. 58, no. 10.
3. K.Jyostna(Asst Prof,VNR VJIET,Hyderabad,India), Dr.V.Padmaja (Prof,VNRVJIET, Hyderabad,India), [2011] ”Secured Embedded System Networking: Advanced Security perspective”-ISSN:0975-5462 Vol 3 No.5
4. Raj S. Katti, , Sudarshan K. Srinivasan and Aida Vosoughi[2011], On the Security of Randomized Arithmetic Codes Against Ciphertext-Only Attacks, IEEE Transactions On Information Forensics And Security, vol. 6, no. 1.
5. Seunghyun Park, Hanjoo Kim, Hichan Moon[2010]”Concurrent Simulation Platform for Energy-Aware Smart Metering Systems”, IEEE Transactions on Consumer Electronics, Vol. 56, No. 3
6. Dae-Man Han and Jae-Hyun Lim Member,[2010] “Smart Home Energy Management system using IEEE 802.15.4 and Zigbee” published in IEEE
7. Xavier Perez-costa and Daniel camps Mur, NEc laboratories Europe [2010] “IEEE 802.11E QOS and Power saving Features Overview and Analysis of combined performance” published in IEEE on Wireless communications.
8. A.Vijayaraj and R.Saravanan, Associate Professor Saveetha Engineering college [2010,]” Automated Eb Billing System Using Gsm And Ad-Hoc Wireless Routing” published in International Journal of Engineering and Technology Vol.2 (5), 343-347.
9. Masa-aki FUKASE(Graduate School of Science and Technology, Hirosaki University) and Tomoaki SATO(c & c Systems center, Hirosaki University Pike Research)[2009], “Compilation Techniques Specific for a Hardware cryptography-Embedded Multimedia Mobile Processor” Smart meter installations to reach 250 million worldwide by 2015,”
10. Goce Jakimoski and K. P. Subbalakshmi, Member, [2008]“cryptanalysis of Some Multimedia Encryption Schemes” published in IEEE transactions on Multimedia vol.10,No.3.
11. M. LeMay, G.Gross, c.Gunter, and S.Garg, University of Illinnois, Urban campaign[2007] “Unified architecture for large-scale attested metering” in Hawalian International conference on System Sciences,Waikoloa Hawaii
12. Masa-aki FUKASE(Graduate School of Science and Technology, Hirosaki University) and Tomoaki SATO(c & c Systems center, Hirosaki University) [2006] “Innovative Ubiquitious cryptography and Sophisticated Implementation” published in IEEE.
13. Brent K.Ducan and Bruce G.Bailey [2004] ”Protection, Metering, Monitoring, and Control of Medium Voltage Power Systems” published in IEEE transactions on Industry Applications vol.40.No.1.
14. Article regarding Government notification in Dinamalar Newspaper “மின் திருட்டு இனி கிடையாது ”,A new meter reading scheme[2012].