International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 5, No.4 (July -2016)

http://dx.doi.org/10.12785/ijcds/050404

Utilization of Mobile Agents for Building a Secure Decentralized Energy System with Remote Monitoring

H. M. Eldegwi [1], M.B. Badawy [2], and Hamdy M. Kelash [3]

[1,2,3] Dept. of Computer Science & Eng., City Faculty of Electronic Engineering, Menoufia University, Egypt

Received 28 Jan. 2016, Revised 30 May 2016, Accepted 15 Jun. 2016, Published 1 July 2016

Abstract: systems have failed in remote rural areas due to weak infrastructures; roads between urban habitations are in a very bad condition even if found, scattered communities and high losses, this makes grid extension not feasible from financial point of view. Decentralized-energy system (DES) is considered the most successful types of rural electrification solutions, especially in emerging countries. Decentralized energy system plans a significant role for developed countries in attenuating risks and security threats of the electricity sector and guarantee continuous electricity distribution in times of natural disasters and attacks. In fact, only decentralized energy supply system can't mitigate with the risk associated with a centralized electricity sector especially in remote rural areas. Therefore, it is urgently required to build a secure model of decentralized energy system integrated with information system for remote monitoring based on mobile agents (MA), and incorporates (RC5) algorithm into the system because of its exceptional simplicity which makes it easy to implement and analyze operational data remotely.

Keywords: Centralized and decentralized; Renewable energy; Microenergy; Mobile agent; Remote monitoring; Security threats; (RC5) Encryption and decryption algorithm.

1. Introduction

Energy system is the backbone of economies and way of life for developed and emerging countries. Obstacles to the electricity supply to remote rural areas does not only hurt the economy and harm the bottom line; but also can cause loss of life and impede the country's ability to respond to large-scale disaster. Decentralized Microenergy (DME) system is an alternative electrical energy supply system which successfully covers the energy demands of remote rural areas. It assures a stable and uninterrupted power supply for typical appliances of households and small businesses whether on-grid, off-grid or transitioning to a grid connection. Overshadowing any discussions on energy supply system is the new sounding word "decentralized energy system". Decentralized energy, is the energy production near to the consumption places, differ than large power plant which sent the production through the national grid. Local generation effectively reduces transmission losses and lowers carbon emissions.

Security of supply is increased at the national level and the customer doesn't have to participate in the offer or reliance on relatively few, large and remote power plants. Long term decentralized energy can offer more competitive prices than traditional energy. While initial installation costs may be higher, a special decentralized energy tariff creates more stable pricing. A decentralized renewable energy system has many environmental and security benefits for households level and different business activities, decentralized energy is the cost-effective route to achieving carbon targets. Low carbon energy savings gives the opportunity to consolidate and sustainable energy option provided locally. This improves the competitive and increases variety of intelligent choices [1-4]. Decentralized systems considered to be more energy efficient than centralized systems because the electricity streams through power lines have fraction losses of various factors. This seems obvious in the long-distance as long as the distance the greater the loss. Installing renewable energy sources close to homes and communities will shorter transmission lines. This will decrease overall electricity consumption and lower the cost needed for transmission lines extension and increase grid efficiency. [5]

In order to reduce complexity and improve dependability in any DME or distributed energy system, we need to apply a decentralized approach where the

E-mail: hossam_mfe@hotmail.com, mbmbadawy@yahoo.com, dr.hamdykelash@yahoo.com

(MA) is the best alternative of the centralized systems. (MA) is object oriented software code that acts on behalf of a customer or system provider. A (MA) is a computer program that is capable of migrating autonomously from node to another, across a heterogeneous network to perform some tasks on behalf of the user. By using (MA) a customer or system supplier can simply launches a (MA) consisting of code, data and other necessary parameter for a specific purpose, and then disconnects. The agent can navigate autonomously through the heterogeneous networks, interacting with many different nodes or other agents, as it processes the desired information and accordingly applied the related actions. The (MA) migrates from one node or individual microenergy system to another while carrying in-between results. This eliminates the need for the client to maintain a network connection while its agents access and process information [6, 7].

This feature has been substantiated to be useful for many applications like remote monitoring and controlling for decentralized energy supply system installed in remote rural areas based on operational data transfer via a mobile network, which have limited or low bandwidth. The repeated communication between the central information system and the remote installed micro-energy systems in case of microgrid infrastructure (Administration remote monitoring system and customer node) collaborations are therefore reduced to an agent transfer operations, sending an operational data and returning with final feedback and accordingly applied a real time action to protect system from misuse or behaviors by the customer like overloads [8, 9].

In this paper, we incorporates (MA) paradigm to implement a decentralized microenergy system instead of using a centralized system, with a security model that is based on (RC5). It is shown that (RC5) block cipher algorithm can be implemented efficiently for encryption of real-time applications and demonstrated that the (RC5) block cipher algorithm is highly secure from the strong cryptographic viewpoint. This ensures the confidentiality of network management agents. These features provide faster well as memory and process savings [10, 11]. Rural remote areas are suffering from lack of electricity supply, which badly affect the development and the standard level of such communities, even it is not included in the future development plan for grid extension which done by the local governments of these countries . Table (1) shows the high increase in amount of energy demands in Middle East and North Africa in the last decades. The conventional energy solutions using fossil fuel increases the problem. However, renewable energy solution emerges as it can help in providing broad energy supply and at the same time reducing GHG emissions [12].

Table 1: Energy demand in MENA Region in Mega tonne of oil equivalent (Mtoe). Source: World Bank.

Year / Region	2003	2010	2020	2030	2003 to 2030
North Africa	124	160	213	262	2.80%
Egypt	53.9	68.2	87.8	108.6	2.60%
Algeria	33	42.5	57.9	69.7	2.80%
Libya	18	25.3	35.9	46.2	3.60%
Others in North Africa	19	24.2	31.5	37.5	2.60%
Middle East	446	597	807	963	2.90%
Saudi Arabia	130.8	181	246.8	289.1	3.00%
United Arab Emirates	39.2	54.3	71.8	84.4	2.90%
Kuwait	22.9	30.2	41.1	48.7	2.80%
Qatar	15.2	31.9	59.4	67.3	5.70%
Iraq	25.8	35.3	47.4	62	3.30%
Iran	136.4	172.9	224.8	271.5	2.60%
Others in Middle East	75.5	91.7	115.5	139.5	2.30%

2. Problem Description and Analysis

However the decentralized energy system (DES) is considered to be a potential sustainable solution for rural areas in developing countries, as it supplies the main demands of human beings of electricity supply. DES faces many challenges in those particular areas e.g. secure operation of installed system due to remote distance, poor infrastructure, low education level and lack of technicians. The integrity of operation data transferred through a communication medium and confidential of financing and e-paying process. Therefore, developing a new approach based on mobile agent is urgently required to give much of its potential away to improve all dimensions of sustainability. The centralized architecture for energy generation and supply causes some problems as follows [13]:

1. Centralized system is not efficient for remote areas energy supply applications due to very large distance and distribution losses in case of grid extension. In addition to high cost.
2. Centralized energy supply system can't mitigate to risks and security threats of the electricity sector and ensuring continuous electricity delivery in times of natural disasters or terrorist attacks.
3. Performance of centralized network degrades gradually and has a quite efficient in terms of performance especially for remote monitoring. It is also badly affected the functionality of the service or system healthy due to huge traffic and data transfer through the mobile network.
4. Huge amount of network traffic at administrator remote monitoring station, which creates extra burden on administrator.
5. System suffers from low performance due to a lot of communication between system remote monitoring administrator and installed energy supply system and vice versa.

6. Bandwidth Limitation of the mobile network.
7. Although the mobile agent (MA) is the best alternative approach of centralized system because of its rich properties mentioned before, there are some downsides concerning the security threats.
8. While the development of decentralized system is necessary to renovate the electricity market and integrate renewable energy. Focusing on decentralized system alone will not mitigate the risk associated with a centralized electricity sector especially for rural remote areas. Using decentralized ME systems in rural areas makes it more difficult in many ways to take advantage of the potential of achieving sustainability. One side is weak infrastructure and long undeveloped roads to individual customers even if found.
9. The operational data, customer's information and e-payment methods for decentralized system suffering risks and security threats of guarantee continuous electricity supply in case of misuse or external attacks.
10. The problem of managing and operating of decentralized system in such area characterized with very poor infrastructure and low education level. This makes decentralized system very weak and vulnerable to many security attacks and threats. This security attacks can changes the operational settings for system components like battery charge and discharge level, the system designed loads. This will continuously damage the system gradually.

3. Limitations of Decentralized Systems

In this section we will summarize the participations and limitations of decentralized systems e.g. microenergy systems for contributory energy supply in remote rural areas.

A. Rural Electrification

About 1.4 billion people all over the world suffering from lack access to electricity and reliable energy supply; nearly 85 percent of them live in the rural areas of developing countries. For example they are suffering from lack of access to electrical efficient light, sufficient energy supply for their household and economic activities, also access to modern information and communication media. On other hand, nearly 2.7 billion people still basically depend on the traditional methods using biomass in the forms of wood, charcoal for cooking and heating [14,15].

Extension of centralized grids is still the biggest challenge due to expensive costs, and high power losses for long distance. However, renewable energies are an affordable and economically viable option to react to the electricity needs of people live in rural remote areas in developing countries and millions of households are being supplied by renewable energy from different sources.

According to Figure 4.1, the world average for transmission and distribution losses in the year 2011 have been estimated to stand at 8.1 percent of the total electricity output, this is according to the World Bank. Electric power transmission and distribution losses include the losses in transmission between sources and distribution points; also form distribution points or substations to customers, including the stolen. This figure rises to a staggering 15.1 percent for the developing countries in MENA Region, 16.1 for the least developing countries and 10.6 for Egypt for the same year [16]. All of these problems limited applying ME systems in a wide rage.

All of these circumstances increase the difficulty and costs for the product providers to ensure save transportation, delivers of system components and hardly offer the required periodic visits for applying the regular services and maintenance. Due to all of above mentioned reasons these remote areas with minimal infrastructure become unattractive for people to live and work especially for high educated people like teachers and doctors, which affect badly on the region investment and development [14-16].

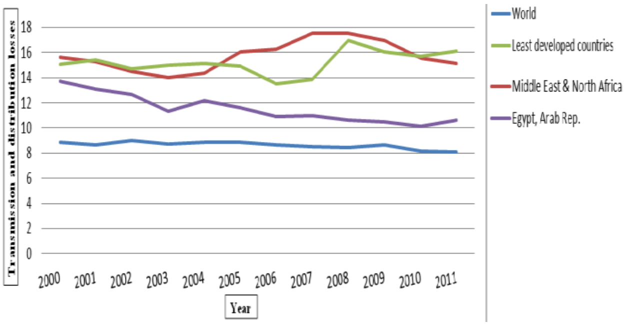


Figure 1. Electric power transmission and distribution losses (% of output) [16]

B. Data integrity and confidentiality

The current energy system infrastructure, which follows the centralized approach architecture is quite efficient in terms of performance and facilitate the intruder mission to storm this centralized system, this affected badly system functionality or continuously of service provision.

A lot of studies show that installed technologies are not protected against components failure or low performance functionality due to security threats and lack of integrity and confidentiality of operational data. One of the widely spread technology in rural areas is Solar Home System (SHS), which often has problems of capacity due to modification of design loads and layout of the installed systems, misuse by the end users or external security threats to change the operation settings to make system components fail. The system performance is badly affected and threated. This leads in some cases to power blackout due to any external corruption or modification to system configuration or data setting for microgrids connection or interface connection.

Microgrids can be used as a backup for the grid in case of any shortage or unexpected outage. ME systems remote central database and information system are vulnerable to any changing or modification [17].

C. Short life time

Lack of communication between all involved project stakeholders or parties like manufacturers, provider, supplier or customer affected the system life span.

It is not necessarily that systems tested under laboratory conditions in manufactory to work fine in real field due to different environmental conditions, misuse and lack of maintenance. Figure 4.2 shows the seven different stages, starting with the production of each component as first of these. After system integration and pre-sale activities such as testing and marketing, the product shifts from the seller to the end-user at the point-of sale. Then, the SHS is sized accordingly, put into operation at the use-stage and needs after-sales services until the components are disposed of on life cycle completion.

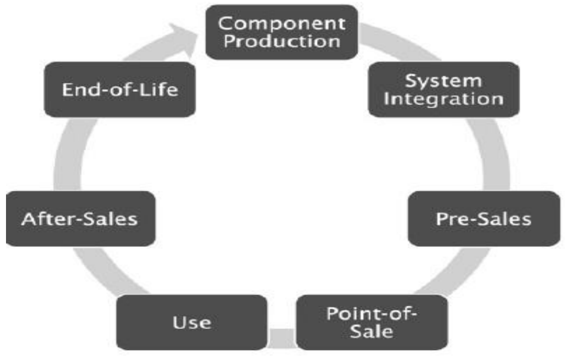


Figure 2. Lifecycle view of a solar home system [18].

Figure 4.3 shows the problem along life cycle of installed SHS, this thesis will focus on solving the main problems concerning the lack of monitoring and insufficient maintenance due to very large distance. This will be achieved through a novel proposed solution, which enable remote monitoring, detect system performance, and prevent misuse of the system, by the end user.

All of these reasons affect badly on the system life time. It is very difficult and not cost effective to send technicians to remote areas, due to long distance, very bad infrastructure and roads difficulty. This increases the difficulty to secure a regular system inspection, schedule services and spare parts availability [18].

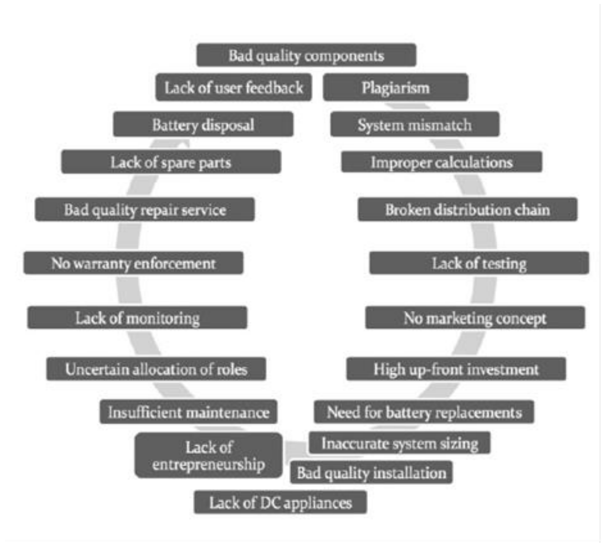


Figure 3. Focus problems along the life cycle [18].

D. Securing financing process

The micro-financing models strongly linked to implementation of ME supply system, especially for households in rural areas with people of lower incomes.

The financing program applied for decentralized energy system, a secure system should be applied for microfinance process to guarantee the e-paying and the credit back, while the information for payback period of the credit are encountered and continue for e-paying their credit instalments which will need to be protected and secured during the e-transaction, taking into consideration customer data integrity and confidentiality.

Summarizing some of the challenges of implementing ME supply systems in remote areas raised the demand for an urgent need for development of an efficient model for building a secure decentralized energy supply system with remote monitoring by using mobile agent [19,20].

4. MICROENERGY SYSTEMS

MES includes a decentralized electrical supply system such as photovoltaic (PV) solar panels, small wind turbines and traditional diesel generators or a hybrid of two or more according to the design principle. Furthermore, it can be also energy storage as batteries or water tanks and energy consumption connectable appliances as efficient lighting, TV, fridges, mobile phone charger, small water pump or fan. This shows the diversity and flexibility of MES as a decentralized electricity supply systems [21-24]. Figure 4.4 shows a traditional schematic for ME system, which is a generalization of a ME source that provides a basic electricity supply on household level and small or medium business [21-24].

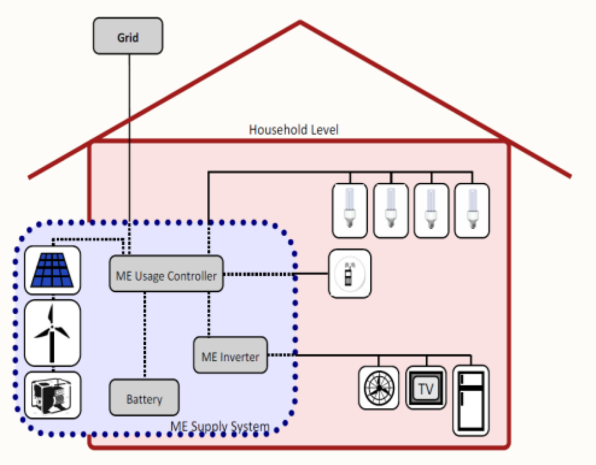


Figure 4. Schematic architecture of existing microenergy system [21]

This example for a traditional model for decentralized system is not efficient or effective for remote rural areas especially in emerging countries due to the above mentioned problems and poor infrastructure in such areas. It is also shortage the system life cycle and hardly enables monitoring the system and determining the problem to avoid the service cut-off or failure. [21-24].

5. Security Reqirements

Our proposed model incorporates MA with RC5 encryption, decryption algorithm for building a secure decentralized energy system with remote monitoring which have the ability to meet the following security requirements [25, 26]:

1. Applying decentralization approach based on MAs for remote monitoring and secure of operational data transfer via mobile network as an alternative solution of the more prevalent centralized system, this to solve the problem caused by the centralized system and to match the natural of the remote rural areas.

2. Data confidentiality: only the agent launched by the system suppliers or system administrator can obtain the data collected by the MA from ME systems or customers through the visited MA during its migration.

3. Non-repudiation: No end user or customer, whom MA has run on, can deny the feedback message or action generated on it or the fact of agent's passing through.

4. Anonymity: for some certain purpose concerning system misuse or delay in monthly instalments pay, no customer knows the migration path of the MA.

5. Integrity: if malicious threats modify the transfer system operational data, even part of it concerning a specific user for certain purpose, mechanism can detect illegal alteration or modification of transferred data.

6. Characteristics of Mobile Agent

MA shall enjoy several of the characteristics. It should enjoy the following compulsory properties: Sensitive and responsive: it senses changes in the environment and acts in accordance [25, 26].

1. Autonomous: it has self-control.
2. Target-driven: it is pro-active.
3. Temporally continuous: it executes continuously.

It may enjoy one or more of the following orthogonal properties:

1. Communicative: it can communicate and collaborate with other agents.
2. Mobility: travel from one node to another.
3. Intelligent: adapt and develop their action.

7. Advantage of Mobile Agent

The advantages of MA are envisioned in their significance over the centralized model. Due to many advantages of (MAs) which make them the best alternative solution for solving the problems of centralized systems [25,26]; some of them are summarized below:

1. They reduce the network load: the client server bandwidth problems, reduces repetitive request / response handshake.

2. They overcoming network latency: For critical real-time systems, such latencies are not acceptable. (MAs) offer a solution, since they can be dispatched from a central controller to act locally and directly execute the controller's directions.

3. They encapsulate protocols: When data are exchanged in an e-transaction or a distributed system.

4. They solve problems created by intermittent or unreliable network connections: (MAs) can easily work off-line and communicate their results when the application is back on-line.

5. They adapt dynamically: Mobile agents have the ability to sense their execution environment and react autonomously to changes.

6. They are naturally heterogeneous: Network computing is fundamentally heterogeneous, often from both hardware and software perspectives.

7. They are robust and fault-tolerant. The ability of (MAs) to react dynamically to harmful situations and events makes it easier to build robust and fault tolerant distributed systems.
8. If a host is being shut down, all agents executing on that machine will be warned and given time to dispatch and continue their operation on another host in the network.

So, it is necessary to utilize the advantages of the mobile agent to adapt agent architecture for applying decentralization approach on e-transaction or distribution system like (dangerous real time systems, decentralized energy, e-transaction...etc.) systems.

8. PROPOSED SOLUTION

This thesis presents a secure decentralized ME supply system with remote monitoring, which suites the natural of remote rural areas based on of mobile agent architecture.

The process started by collecting and recording data via an agent called (MA_ data recording) from ME usage controller. The MA can collect operational data from the first visited node of ME system and continues migration from node to another with the assistance of the Leader agent (LA). The LA is created remotely by system monitoring administrator to help him in performing different management tasks and actions, also LA is controlling or supervision all MAs participating in the transaction. The Static Agent (SA) is launched for the first time by system administrator and restrains at the local network in the field of installed ME systems. It concatenates the operational data collected at each node with the data carried by MA and then the LA encrypts them using RC5 encryption algorithm into an indivisible whole for protection. At the same time LA sends certain information to each partner according to threshold scheme. Then only a certain number of partners can retrieve the node's identity information and report the result to LA.

When the LA finishes the task, then it takes the encrypted operational data and launched with the encrypted data remotely to system administrator. LA reached the system administrator after finishing its migration in order to perform automatic operational data analysis tasks on behalf of its own system provider or supplier, SA will compare the identity information given by its partners with that retrieved from encrypted data to find out if there an attack exists.

Figure 4.5 described the process of data transfer through mobile network using MA under supervision of the LA. Starting from Remote Monitoring Administrator (RMA) carrying requested operational data for different ME systems of behalf on it's the owner or provider after migrates between different nodes or ME systems (ME1, ME2, ME3……MEn) according to certain principles and back to RMA with the overall operational data for ME implemented systems.

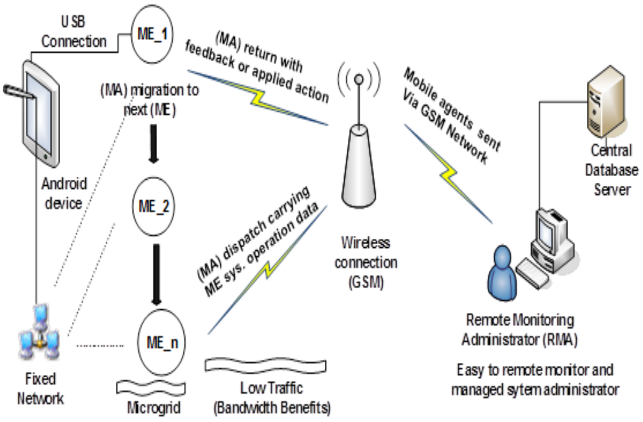

USB Connection
ME_1
(MA) return with feedback or applied action
(MA) migration to next (ME)
Mobile agents sent Via GSM Network
Central Database Server
Android device
ME_2
(MA) dispatch carrying ME sys. operation data
Wireless connection (GSM)
ME_n
Remote Monitoring Administrator (RMA)
Easy to remote monitor and managed sytem administrator
Fixed Network
Microgrid
Low Traffic (Bandwidth Benefits)

Figure 5. Proposal for data transfer process for decentralized energy system through mobile network based on MA

Starting from Remote Monitoring Administrator (RMA) carrying requested operational data for different ME systems of behalf on it's the owner or provider after migrates between different nodes or ME systems (ME1, ME2, ME3……MEn) according to certain principles and back to RMA with the overall operational data for ME implemented systems.

9. MICROENERGY SUPPLY SYSTEM BASED ON MOBILE AGENT(MEMAS)

The central data is created on a remote central server; it is designed for storing and analysing the collected system operation data, including detailed information concerning all the customer information and load design, method of payment, and all technical data and settings which is important for remote monitoring and services. Figure 4.6 shows architecture of the proposed model [27].

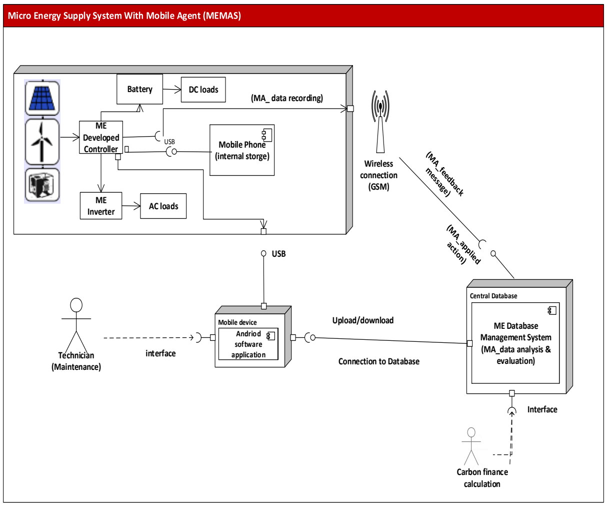
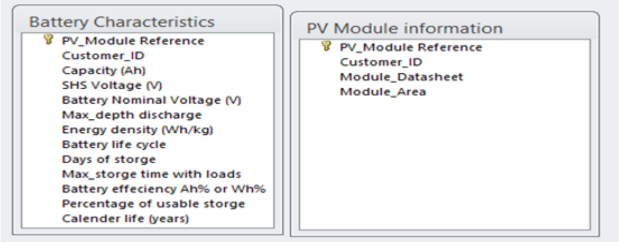


Figure 6. The architecture of the developed model for decentralized ME.

The second level of data access is designed for the local supplier of the SHS, and finally the customer view. All the above mentioned hierarchically level of access data are started from the first level which enable all parties according to involved in this level to fully access the database [27].The second level enable access to some specific data concerning information and data like the technical level which is important for the local provider to ensure the services and required repair, and finally the last level for the customer accesses concerning information like the loads and the monthly instalments.

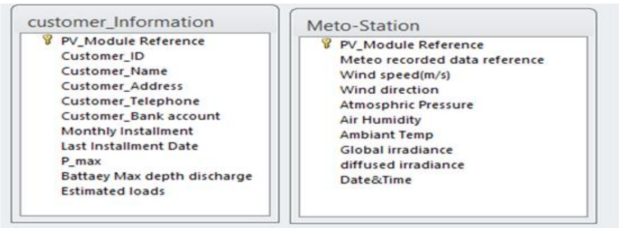
Figure (4.7), (4.8), (4.9), (4.10) shows the central database estimated relational tables structure built.



Battery Characteristics
PV_Module Reference
Customer_ID
Capacity (Ah)
SHS Voltage (V)
Battery Nominal Voltage (V)
Max_depth discharge
Energy density (Wh/kg)
Battery life cycle
Days of storge
Max_storge time with loads
Battery effeciency Ah% or Wh%
Percentage of usable storge
Calender life (years)

PV Module information
PV_Module Reference
Customer_ID
Module_Datasheet
Module_Area

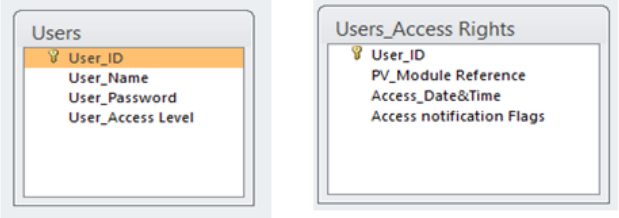
Figure 7. Storage characteristics and PV module information



customer_Information
PV_Module Reference
Customer_ID
Customer_Name
Customer_Address
Customer_Telephone
Customer_Bank account
Monthly Installment
Last Installment Date
P_max
Battaey Max depth discharge
Estimated loads

Meto-Station
PV_Module Reference
Meteo recorded data reference
Wind speed(m/s)
Wind direction
Atmosphric Pressure
Air Humidity
Ambiant Temp
Global irradiance
diffused irradiance
Date&Time

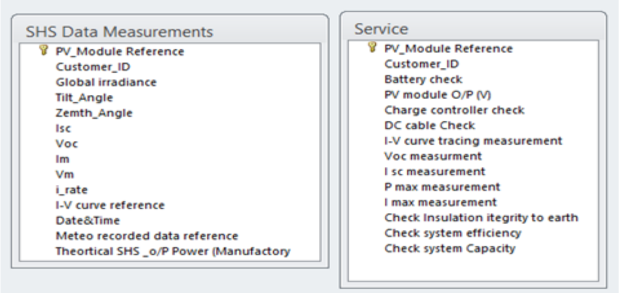
Figure 8. Customer profile and meteorological data



Users
User_ID
User_Name
User_Password
User_Access Level

Users_Access Rights
User_ID
PV_Module Reference
Access_Date&Time
Access notification Flags

Figure 9. User identification and stakeholders’ access level



SHS Data Measurements
PV_Module Reference
Customer_ID
Global irradiance
Tilt_Angle
Zemth_Angle
Isc
Voc
Im
Vm
i_rate
I-V curve reference
Date&Time
Meteo recorded data reference
Theortical SHS _o/P Power (Manufactory

Service
PV_Module Reference
Customer_ID
Battery check
PV module O/P (V)
Charge controller check
DC cable Check
I-V curve tracing measurement
Voc measurment
I sc measurement
P max measurement
I max measurement
Check Insulation itegrity to earth
Check system efficiency
Check system Capacity

Figure 10. Tables structure for SHS operation data and applied services

10. THE MAIN FUNCTION OF MOBILE AGENTS

1. Leader Agent (LA): LA is a mobile agent which was created by system administrator to lead the entire MAs for each individual ME systems to finishes the task through migration among MEs on behalf of its customer or owner, also it help network administrator to launch other agents Configuration Agent (CA), Partner Agent (PA), and (IP & Controller serial) Agent. Then collect data required for remote monitoring and managing the system. The LA is responsible for encryption of the data collected by the MAs after finishing its task on MEs, and then leads the MAs in its trip to remote central database.

2. Static Agent (SA): It stays or resides at each local network in the field of MEs to help LA finishing required tasks.

3. Partner Agent (PA): Partner agent is responsible for deciding the MEs nodes which will be visited by the MAs on the basis of a list generated or defined through a mechanism of specific addresses of IP-controller serial to address MEs nodes which will be visited , then it prepares the lists and sends it to the RMA as follows:

4. Matched List-: list all the connected MEs or customers with correct pairs of IP and controller serial

5. Unmatched List-: list all the MEs or clients with different IP and controller serial than those assigned to them.

6. (IP & Controller serial) Agent: this agent is launched by system administrator under supervision of LA to test the connectivity with the installed ME system. The IP& controller serial agent reaches the remote ME controller if it is running and active or working properly.

7. Configuration Agent (CA): is responsible to check the configuration of ME system installed in remote rural area and return back with results or feedback to system administrator. Configurations of remote ME system include for example data about the connected loads, battery charging level and the status of the charge controller at remote customer own system. These configuration items help system administrator to learn about various loads running. If any unauthorized or misuse is found then he reports a warning message to the end user to disconnect extra loads and in case not responding within a margin time a remote disconnection can be applied by connecting the controller and disconnect extra loads. This property of remote connection and applied action by sending MA via mobile network in a real time response will affect system performance, operation

data integrity and reduces the fault tolerance especially for real time applications. The agents IP& controller serial and Configuration agent (CA) is just for helping the system administrator to finish his schedule tasks like remote monitoring and managing ME systems.

11. Operation Data Analysis

Mobile agents are used to make the following calculations, analysis and applied actions or response according to system technical boundary conditions and under supervision and control of LA. Figure 4.11 shows the mobile agents analysis process and boundary conditions for SHS.

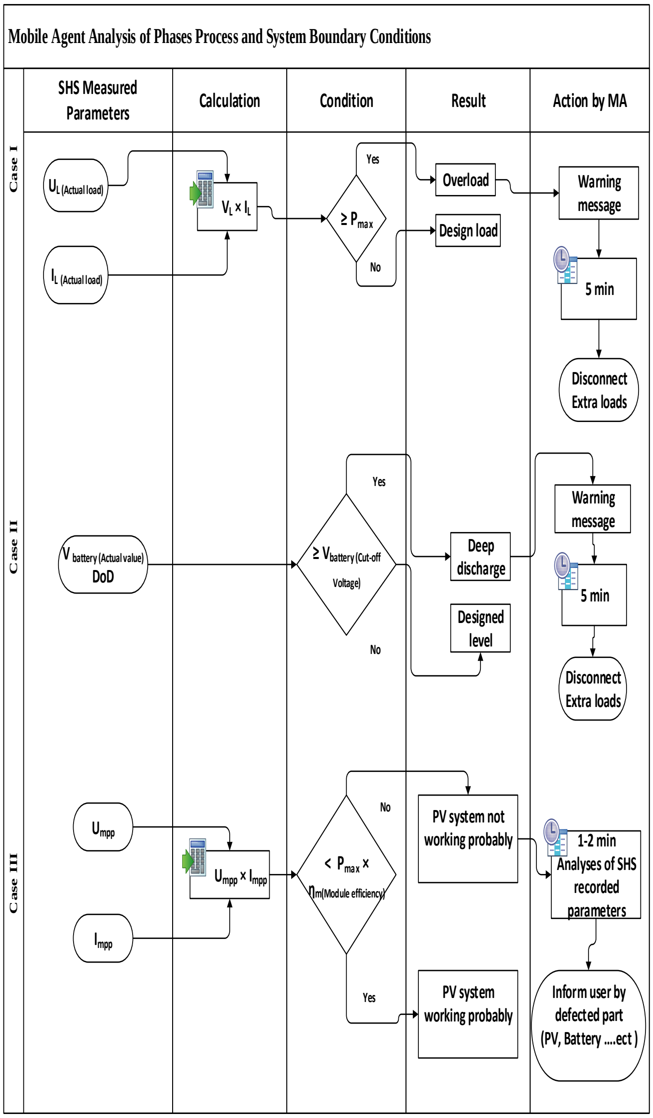


Figure 11. Cross function flowchart of mobile agent analysis process and boundary conditions for SHS

The processes are divided into three cases as follows:

Case I

1. The mobile agent measures the input parameters inputs of Voltage and current load (VL & IL)
2. Mobile agent analysis & calculations for comparing the values VL *IL with power reference in the datasheet Pref
3. If (VL *IL ≥ Pref), then the (MA_feedback) will define the case and send a message with (Overload).
4. (MA_applied action) will send a warning message to the customer and if the customer continued with the overload a disconnection to extra loads will be done remotely.

Case II

1. The mobile agent measures the battery voltage (Vbatt)
2. Mobile agent analysis & calculations for comparing the values measured (Vbatt) with the reference discharge voltage of the battery (Vref_min_discharge)
3. If (Vbatt ≤ Vref_min_discharge), then the (MA_feedback) will define the case and send a message with (Battery deep discharge).
4. (MA_applied action) will send a warning message to the customer and if the customer continued with the overload a disconnection to extra loads will be done remotely.

Case III

5. The mobile agent measures the maximum voltage and current of the PV system (Vmax & Imax) and (Pmax & ηpv) , where ηpv is the efficiency of the PV system.
6. Mobile agent analysis & calculations for comparing the values measured (Vmax * Imax) with (Pmax * ηpv).
7. If (Vmax * Imax) << (Pmax * ηpv). , then the (MA_feedback) will define the case and send a message with (PV system not working probably).
8. (MA_applied action) will send a message to the customer asking him to perform a visual check for the system (PV, Battery .etc.).

12. CO_2 EMISSION CALCULATIONS USING MA

MA can play an important role in performing the process for evaluating operation data, which includes some tasks concerning the creation of the profiles for end users, calculation of CO2, defining the status of the system and preparing important statistics required for future design improvement. Figure 4.14 shows the evaluation process of operation data using mobile agent.

For the lighting system specifically for the baseline case of kerosene, table (2) shows the following parameters stored in the database and used by the mobile agent for calculating baseline emission from lighting of one example of customer household, the end user can benefits from selling the emission certificate to an organization and the money earns can help in improve the user income an alleviate in his monthly payment [28]:

$$\mathrm{LEF} = \mathrm{FUR} \times \mathrm{LUR} \times \mathrm{AU} \times \left(\frac{\mathrm{EF}}{1000}\right) \times \mathrm{LF} \times \mathrm{N} \times \mathrm{NTG} \times \mathrm{NH}$$

Table 2: Lighting systems emission calculation parameters

Parameter	Unit	Description	Value
LEF	[tCO_2e /project lamp]	Lamp Emission Factor	tCO_{2e}/lamp*y
FUR	[l/h]	Fuel use rate	0.025 l/h
LUR	[h/d]	Lighting utilization rate	8 h/d
AU	[d/y]	Annual utilization	365 d/y
EF	[$kgCO_2$/l]	Fuel emissions factor	2.5 $kgCO_2$/l
LF	--	Leakage factor	1
N	--	No. of fuel-based lamps replaced per Project Lamp	3
NTG	--	Net-to-gross adjustment factor	1
NH	--	No. of Households	1

An appropriate mobile agent will automatically make the calculation for the estimated customer according to his profile and stored operational data as follows:

$$\mathrm{LEF(houshold)} = 0.025\left(\frac{\mathrm{l}}{\mathrm{h}}\right) \times 8\left(\frac{\mathrm{h}}{\mathrm{d}}\right) \times 365\left(\frac{\mathrm{d}}{\mathrm{year}}\right) \times \frac{2.5}{1000}(\frac{\mathrm{tCO2}}{\mathrm{l}}) \times 1 \times 3 \times 1 \qquad (1)$$

By the end an emission certificate will be created by the following value:

$$\mathrm{LEF}(\text{one houshold}) = 0.548(\frac{\mathrm{tCO2e}}{\mathrm{lamp.Year}}) \qquad (2)$$

13. ENCRYPTION AND DECRYPTION ALGORITHM

The description of the encryption algorithm is given below. Here, we assume that the input block is given in two W-bit registers A and B, and the output is placed in the registers A and B. The decryption routine is easily derived from the encryption routine [10, 11].

1) (RC5) uses three mathematical operations:
   - Two's complement addition.
   - XOR.
   - Left cyclic rotation by variable amounts.
2) These are all fast operations that are directly supported by most modern processors.
3) Parameters: K (key), w (word length), r (number of rounds)
4) Input: a 2w length plaintext in registers A and B.
5) Output: a 2w length ciphertext.
6) Expand K into a table S [2(r+1)] keys.
7) To encrypt:
   - A =A + S [0]; B = B + S [1]
   - For i = 1 to r $\mathbf{d_o}$
   - A = ((A xor B) << B) + S [2 * i]
   - B = ((B xor A) << A) + S [2*i + 1]

8) Decryption steps are the same but in reverse.

(RMA) will reserve one pair of encryption key and description key using (RC5) encryption, decryption algorithm which is not known by any of the system parities. We call them (RC5e) and ($RC5_d$), the (RC5e*)* is used to encrypt data carried by MA reaches or connected to the microenergy usage controller ME.

14. MAIN STEPS OF THE PROPOSED SOLUTION

- System administrator Task: The (RMA) generates a leader agent (LA) which leads the (MAs) with different requests to execute a specific tasks on behave of its end users or the customer on a remote (MEs) in order to protect system components and prevent misuse. The (MA) will reach remote ME destinations according to current network environment by the help of the partner agent (PA) as described before, and decide which is the first node that it will be visited according to the matched list created by RMA . Supposing that the (MA) will start by first node (ME1), then counts:

$$D_{RMA} = RC5_{Enc.pb(SA)}\left(Sign_{pri(\mathrm{RMA})}\left(d_{RMA}\right)\right) \tag{3}$$

- The (RMA) uses its private key to sign on (d_{RMA}) which represents its request, then it will be encrypted by the public key generated by (SA) using (RC5) algorithm ($RC5_{Enc.pb(SA)}$), the (SA) works here as a trusted third party (TTP) to form finally (D_{RMA}) which will be send to (ME1) controller. Where:

d_{RMA} represent the request by (RMA) and carried by (MA) under supervision of (LA) to execute a operational data collection or perform applied action and it is signed by (RMA) private key $\left[Sign_{pri(\mathrm{RMA})}\right]$, then count the hash value (h_{RMA}) which denote to the hash value of the data request by (RMA) which will be carried by its own (MA) to finish its specific task on (ME_1) and (LA) will carry it back as follows:

$$h_{RMA} = H\left(Sign_{pri(\mathrm{RMA})}\left(d_{RMA}\right)\right) \tag{4}$$

$$D'_{RMA} = D_{RMA} \parallel h_{RMA} \tag{5}$$

- Leader Agent Migration: The (LA) which was created by the remote monitoring system administrator (RMA) will start its migration from (RMA) station or server to first node or (ME) system with the (MA) carrying the requested data $\left(D'_{RMA}\right)$.
- Now the (LA) decides which is the first node or (ME) systems according to the pre-select list by (RMA) here we suppose that the first node is (ME1). (ME1) will receive the (LA) migrating from (RMA) station with the data $\left(D'_{RMA}\right)$. The (LA) launches the (MA) which own request to finish a specific task on (ME1), then it generates data (d1) and determines its next node (ME2) according to current network environment. The (ME) systems or nodes being visited uses its private key to sign on the original operation trusted data that represent the real operation status without any modification (d), concatenates (d1) with (ME1) and $\left(D'_{RMA}\right)$, then encrypts by the (SA) public key using (RC5) algorithm then:

$$D_1 = RC5_{Enc.pb(SA)}\left(ME_1 \parallel d_1 \parallel Sign_{pri(\mathrm{ME}_1)}\left(d_1\right) \parallel D'_{RMA}\right) \tag{6}$$

After that (MA) computes Hash value:

$$h_1 = H\left(ME_1 \parallel d_1 \parallel Sign_{pri(\mathrm{ME}_1)}\left(d_1\right) \parallel D'_{RMA}\right) \tag{7}$$

Then concatenate (D_1) and (h_1), then we can get:

$$D'_1 = D_1 \parallel h_1 \tag{8}$$

- Then (LA) migrates to next hop carrying data (D'_1).

At the same time the (LA) visit any of the (ME) systems, each one sends its identity information to static agent (SA) resides at (RMA). This process happened only in case of any e-paying or electronic money transfer or request, for example (ME1) will send its identity information after signing it with its private key to the (SA) immediately when he receives the (LA) as follows:

$$RC5_{Enc.pb(SA)}\left(Sign_{pri_{(\mathrm{ME}_1)}}\left(ME_1\right)\right) \tag{9}$$

- When data received, the static or stationary agent (SA) can obtain the nodes or (ME's) identity information through decryption as follows:

$$RC5_{Dec.pri(SA)}\left(RC5_{Enc.pb(SA)}\left(Sign_{pri_{(\mathrm{ME}_1)}}\left(ME_1\right)\right)\right) \tag{10}$$

1- Leader agent (LA) migrates to service host (ME_i) :

- When the (LA) reaches (MEi); with data (D'_{i-1}), then chooses its next node hop $(ME_{i+\mathbf{1}})$ according to current network environment. (ME_i) signs on (d_i) with its private key, concatenate (ME_i), $(ME_{i+\mathbf{1}})$, (d_i) and (D'_{i-1}) to form:

$$D_i = RC5_{Enc.pb(SA)}\left(ME_i \parallel ME_{i+1} \parallel d_i \parallel Sign_{pri(\mathrm{ME}_i)}\left(d_i\right) \parallel D'_{i-1}\right) \tag{11}$$

Then compute Hash value:

$$h_i = H\left(ME_i \parallel ME_{i+1} \parallel d_i \parallel Sign_{pri(\mathrm{ME}_i)}\left(d_i\right) \parallel D'_{i-1}\right) \tag{12}$$

- After that Concatenate (D_i) and (h_i) to form:

$$D'_i = D_i \parallel h_i \tag{13}$$

Then (LA) migrates to next hop with encrypted data $\left(D'_i\right)$, Meanwhile, (ME_i) sends its identity information to (SA) as follows:

$$RC5_{Enc.pb(SA)}\left(Sign_{pri(\mathrm{ME}_i)}\left(ME_i\right)\right) \tag{14}$$

(SA) can obtain $(ME_i\text{'s})$ identity through decryption and certificating signing when receives data above:

$$RC5_{Dec.pri(SA)}\left(RC5_{Enc.pb(SA)}\left(Sign_{pri_{(\mathrm{ME}_i)}}\left(ME_i\right)\right)\right) \tag{15}$$

- The leader Agent (LA) returns to (SA), it is assumed that the (LA) returns to (SA) after passing throw the node or server (MEn) according to the pre-generated matched list, now (LA) is carrying with data (D'_n).

$$D'_n = D_n \parallel h_n \tag{16}$$

$$D'_n = \left[RC5_{Enc.pb(SA)}\left(ME_n \parallel SA \parallel d_n \parallel Sign_{pri(\mathrm{ME}_n)}\left(d_n\right) \parallel D'_{n-1}\right)\right] \parallel \left[H\left(ME_n \parallel SA \parallel d_n \parallel Sign_{pri(\mathrm{ME}_n)}\left(d_n\right) \parallel D'_{n-1}\right)\right] \tag{17}$$

- The (SA) retrieves (D_n) and (h_n) through (D'_n) as *(SA)* decrypts (D_n) using its private key. Operating the hash function on decryption result, then compare hash value with (h_n), if they are same to each other, we can be sure that data has not been changed or modified .
- Then the (SA) decrypt (D_{n-1}), continue to this proceed. If hash value is different from equivalent (h_i), we can say that the data has been modified. After finishing the decryption, (SA) can obtain data compilation (compilation_data) and address compilation (compilation _add$_1$) as follows:

$$compilation\_data = \{d_{RMA}, d_1 .... d_n\} \tag{18}$$

$$compilation\_add_1 = \{ME_1, \mathrm{ME}_2 .... \mathrm{ME}_n\} \tag{19}$$

- Meanwhile, (SA) receives identity information from each visited (ME) system immediately after the (LA) agent leaves:

$$\begin{array}{l} RC5_{Enc.pb(SA)}\left(Sign_{pri_{(\mathrm{ME}_1)}}(ME_1)\right), \\ RC5_{Enc.pb(SA)}\left(Sign_{pri_{(\mathrm{ME}_2)}}(ME_2)\right), \\ . \\ . \\ RC5_{Enc.pb(SA)}\left(Sign_{pri_{(\mathrm{ME}_n)}}(ME_n)\right) \end{array} \tag{20}$$

- Through decryption and certificate signing on data above, (SA) can obtain address compilation (complition_add2) as follows:

$$complition\_add_2 = \{ME_1, ME_2, ... ME_i .... ME_n\} \tag{21}$$

If (complition_add2) is the same as (complition_add1), modification or damage has not occurred; otherwise data has been modified or damaged.

- The (SA) sends final result to (RMA):
- After steps above, if all the data has not been illegally modified through verify, (SA) encrypts original data and sends them to (RMA), otherwise sends information to show damage when transmission. We use (1) bit to express data received by (SA) is reliable or not. Bit (1) represents success (data received by (SA) is correct), (0) means failure (data received by (SA) has been modified or damaged).
- The two cases described below:

Sending information as below when data has been transmitted correctly:

$$RC5_{Enc.pb(\mathrm{RMA})}\left(1 \| Sign_{pri(SA)}(SA) \| \left(d_1\right) \| ... \left(d_i\right) \| ... \| \left(d_n\right)\right) \tag{22}$$

Sending information as below when data has been damaged:

$$RC5_{Enc.pb(\mathrm{RMA})}\left(0 \| Sign_{pri(SA)}(SA) \| \left(ME_{i_1}\right) \| ... \| \left(ME_{i_n}\right)\right) \tag{23}$$

$If\left(ME_{i_1}\right) \| .... \| \left(ME_{i_n}\right)$ are malicious hosts and make any changes with the operational data or settings. When (RMA) receiving (SA's) data, it decrypts the data with its private key then decide what the results mean according to the one bit (1) or (0). Accordingly to this report the network administrator will take an appropriate action concerning the network management task, also the administrator by the help of this report may deprive the customers who misuse or overload (ME) system applying accountability , penalty or remotely disconnect extra loads.

15. Conclusion

A new approach for building a secure decentralized ME system with remote monitoring based on MA System (MEMAS) was presented. This approach aims to build a secure ME system with remote monitoring, which is efficient and suitable for remote rural areas with poor infrastructures.

It secures a source of sustainable energy supply for remote rural areas, in order to overcome the conventional energy supply systems problems due to large distance and losses in case of electrical grid extension. In addition to very high costs for the electrical grid extension, in some cases like Sinai Peninsula in Egypt, it reaches more than 450 km.

The operation data is collected by MA and transferred through mobile network after encryption process using RC5 to protect operation data and controller settings from being changed or modified.

References

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. (references)

[2] Amsalu, S.,Elmer, M.,Newman, R. and Gashie, W. (2009). Rural Electrification with Photovoltaics, Stiftung Solarenergie-Solar Energy Foundation.

[3] Micro Energy International: Micro-energy systems architecture, http://www.microenergy-international.com/ 20 June 2014.

[4] International Energy Agency – IEA & United Nations Developent Programme – UNDP & United Nations Industrial Development Organization - UNIDO (2010). Energy Poverty - How to make energy access universal? Special early excerpt of the World Energy Outlook 2010 for the UN General Assembly on the Millennium Development Goals. OECD/IEA.

[5] DfID (2002). Energy for the poor – Underpinning the Millennium Development Goals. Department for International Development, London.

[6] Osha Gray Davidson, “Why We Need a ‘Local Energy’ Movement,” Mother Jones, 2 November 2009, http://www.motherjones.com/blue-marble/2009/11/why-we-need-local-energy-movement (29 June 2015).

[7] Jian Hu, Rui Zhao, Xiao-Mei Qui, "A network management model based on mobile agent system" School of Computer Science and Engineering University of Electronic Science and Technology of China, IEEE 2008, pp 279-283.

[8] Muhammad Aiman Mazlan, Azman Samsudin, "Secure Groups Communication For Mobile Agents Based On Public Key Infrastructure". 9th IEEE Asia Pacific Conference on Communication APCC2003.

[9] Eung-Gu You, Keum-Suk Lee, "A Mobile Agent Security Management", Proceedings of the 18th International Conference of IEEE on Advanced Information Networking and Application (AINA'04).

[10] Rivest, R. L. (1995). (RC5) encryption algorithm. Dr Dobbs Journal, 226, 146–148.

[11] Rivest, R. L. (1997). The (RC5) encryption algorithm. MIT Laboratory for Computer Science, 545 Technology square, Cambridge, Mass. 02139 (Revised March 20, 1997). Available at: http://www.researchgate.net/profile/Osama_Allah/publication/225435090_Digital_Image_Encryption_Based_on_the_RC5_Block_Cipher_Algorithm/links/5501547f0cf2aee14b592fec.pdf.

[12] AGECC: Energy for a sustainable future, the secretary-general's. Advisory group on energy and climate Change (AGECC), "Summary report and recommendations", New York, 28 April 2010.

[13] Rafael Wiese, Volker Schacht, PSE AG (2010). Results of the technical and financial monitoring of a micro-financed program for solar home systems in Bangladesh. 25th European Photovoltaic Solar Energy.

[14] Kammen, D. M. &Kirubi, C., "Poverty, energy, and resource use in developing countries", Focus on Africa. Annals New York academic of science, 2008.

[15] Legros et al., "The Energy Access Situation in Developing Countries", United Nation Development Programme, New York, 2009.

[16] World Bank, Electric power transmission and distribution losses (% of output), MENA,http://data.worldbank.org/indicator/EG.ELC.LOSS.ZS. last retrieve on April 2013.

[17] Jian Hu, Rui Zhao, Xiao-Mei Qui, "A network management model based on mobile agent system" School of Computer Science and Engineering University of Electronic Science and Technology of China, pp 279-283, IEEE 2008.

[18] Klara L., "Quality Issues in the Market Based Dissemination of Solar Home Systems", Micro Perspectives for Decentralized Energy Supply (MPDES), Proceedings of the International Conference, Technical University Berlin, 2011.

[19] Kebir, N., "The African electrification initiative, the role of microfinance", Submitted to World Bank Publications, 2011.

[20] Kebir, N., "Manual for the design and modification of Solar Home System components", Micro-energy International. Nieuwenhout, F. D., & Vervaart, M. R., Microfinance & Energy, 2008.

[21] John P. J., Moses M., "Opportunities and challenges for solar home systems in Tanzania for rural electrification", in Technical University Berlin, Micro perspectives for decentralized energy supply, 2011.

[22] Nieuwenhout F., Van D. A., Lasschuit P., Van R. G., Hirsch D., "Experience with solar home systems in developing countries", Progress in photovoltaic research and applications, 2001.

[23] Lindner K., "Quality Issues in the Market Based Dissemination of Solar Home Systems", Micro Perspectives for Decentralized Energy Supply (MPDES), Proceedings of the International Conference, Technical University Berlin, 2011.

[24] Rafael W., Volker S., "Results of the technical and financial monitoring of a micro-financed program for solar home systems in Bangladesh" 25th European Photovoltaic Solar Energy conference and exhibition , 2010.

[25] Buchman W. J., Naylor M. and Scott A. V., "Enhancing Network Management Using Mobile Agents", Engineering of Computer Based Systems (ECBS 2000) Proceedings, 7th IEEE International Conference and Workshop, 2000.

[26] R.Pugazendi, K.Duraiswamy and E.Jayabalan "Intelligent Network Monitoring using Mobile Agent" International J. of Engg. Research & Indu. Appls. Vol.1. No V, pp. 293-306, 2008.

[27] "Microenergy Supply System (MESUS) project", Fraunhofer IPK, Institute for Production Systems and Design Technology, , the concept of solar home systems for rural areas, https://www.ipk.fraunhofer.de/en/homepage/, Berlin, Germany, 2013.

[28] Micro-energy Supply System (MESUS) project; Micro Energy International (MEI) German company: CO2 Emission Reduction Formulas.

H. M. Eldegwi is a Chief Engineer of Projects Implementation Department, New and Renewable Energy Authority (NREA) Egypt.He is a renewable energy professional with over twelve years of experience in renewable energy and energy efficiency in (NREA). He worked as a research assistant in Fraunhofer IPK Institute for Production Systems and Design Technology, Berlin (Germany), for developing Micro-energy supply system for rural off grid areas.

M.B. Badawy is an assistant professor in computer science and engineering department, Faculty of Electronic Engineering, Menoufia University, Egypt. His main research interests include database design, relational database, information security and computer security.

Hamdy M. Kelash is professor in computer science and engineering department, Faculty of Electronic Engineering, Menoufia University, Egypt. His main research interests include computer vision, mobile agent, image processing.