A Smart Residential Security Assisted Load Management System using Hybrid Cryptography

Cristian Chiñas-Palacios[a,c*] (https://orcid.org/0000-0002-1808-1983), Jesus Aguila-Leon[a,c] (https://orcid.org/0000-0003-0538-0842), Carlos Vargas-Salgado[b,c] (http://orcid.org/0000-0002-9259-8374), Edith X. M. Garcia[a], Julián Sotelo[a], Elías Hurtado[b,c]

[a] Departamento de Estudios del Agua y de la Energía, Universidad de Guadalajara, Centro Universitario de Tonalá, Av. Nuevo Periférico Manuel Gómez Morin 555, Ejido San José Tatepozco, 45425, Tonalá, México.

[b] Departamento de Ingeniería Eléctrica, Universitat Politècnica de València,Camino de Vera s/n, 46022, Valencia, España.

[c] Instituto Universitario de Ingeniería Energética, Universitat Politècnica de València, Camino de Vera s/n, 46022, Valencia, España.

ABSTRACT A residential load management system equips smart meters (SMs) to measure load utilization at residencies. SM reports electricity usage based on electronic appliances. In this paper, a smart residential load management system is designed by three-fold along with the provisioning of consumer security. Load management encompasses load categorizing by Hopfield neural network, fuzzy-logic based bill payments identification and load state prediction using Markov chain. Residential load is based on three classes: active load, affordable load and inactive load. The estimation of residential load ensures to manage the load at residency either to turn off the load or intimate excess consumption of electricity. The registered consumers of a specific residency are enabled to receive load status by Internet of Things (IoT) devices. SMs at residencies periodically compute the electricity manipulation and those readings are encrypted using hybrid blowfish and elliptic curve cryptography algorithm with considering the behavior information from IoT device and partial key storage assists security, even if the device is theft. This smart residential security assisted load management (SRS-LM) system is developed in network simulator 3 and the results showed improvements in terms of power usage, load power, peak load reduction, total power consumption, power cost and computation time.

Keywords: household appliances; IoT devices; smart residential, energy meters; cybersecurity; hybrid cryptography.

1. Introduction

Load management in residential sectors is presented to promote the energy savings of household appliances. Smart Meters (SMs) are devices deployed in a residential environment to monitor electricity usages. The measurements from SMs are temporally varied by the changes in load [1]. Home load management is designed as a decentralised framework that is embedded with SMs [2]. The load is scheduled based on the cost variations from the service provider that comforts the customers. The consumption of electricity depends on the characteristics of every home that defines the constructed structure of it. According to variations in size and

counts of the rooms at home, electricity consumption is varied. Among all the available home appliances, some of them consume more considerable energy, whereas others consume comparatively lesser energy [3]. In designing a smart home architecture, the loads are divided based on their utilisation of electricity.

An energy management system in the residential sector is designed to control household appliances to reduce the electricity cost [4]. Considering the load power demand, the payment cost of the customer is determined. This is a potential benefit for the customer, which is attained by designing a two-level residential energy management framework. Increasing electricity demand tends to escalate the energy cost for customers. A smart house management system controls the decisions of household appliances that probably comforts customers [5].

Residential load management system reliability decision based is presented to evaluate customer's participation [6]. Load curtailment function is modelled to minimise the satisfactory level of customer. End-user comfort is provisioned using a heuristic algorithm, i.e. genetic algorithm (GA), for optimal fitness estimation [7], [8].

Controlling household appliances is achieved by GA for reducing energy consumption. User activity level is determined from the usage of appliances as ventilation, air conditioning, and others. Peak load at the residency is minimised with the assistance of Quality of Experience (QoE) based on fuzzy logic controller [9]. QoE is adaptively changed based on the estimated power consumption output (Low, Medium and High) from fuzzy logic.

SMs in collecting electricity measurements support IoT applications based on consumers. Security is a challenging issue that is concerned to ensure privacy techniques [10]. Security provisioning is associated with lightweight authentication and cryptography techniques. This SM involved residential sector is subjected to certain vulnerable attacks. In [11], differential privacy is modelled for distinguishing SMs with privacy providence. Additive Homomorphic encryption is used for protecting the smart meter readings. Encrypting the data from SMs is a solution for ensuring security. Flexible data privacy is essential to appropriately decide on the SM reading [12]. Signature-based encryption is constructed at the gateway device in a residential environment. SM can collect electricity measurements and encrypt the data for security.

Nowadays, one of the challenges in the electricity metering system is the uncertainties about predicting the energy demand for optimal dispatch of a living place [13]. Normally, the utility grid supplies energy to homes employing one of the three phases, making it vulnerable to load imbalance which is caused mainly due to uncertainties. In this scenario, a load management system plays an important role in the electricity distribution for the optimal energy dispatch to the household appliances in residential sectors [14]. The load is scheduled based on the cost variations from the service provider that comforts customers. In a smart home architecture design, the loads must be divided based on the utilization of electricity. According to variations in size and counts of the rooms at home, electricity consumption is varied. Furthermore, it is essential to incorporate a data acquisiton system for monitoring electrical parameters to cover the energy consumed at homes [15]. SMs in collecting electricity measurements support IoT applications based on consumers. On the other hand, user anonymity is vital in

designing a load management system [16]. The monitoring of user load leads to gaining knowledge about user behavior which further leads to potential accessibility of the network by everyone. It has to be considered the security system design for enhancing the load management system by using practical methods to protect user privacy.

The objective of this research work is to design a security assistant load management system using hybrid cryptography. The smart residencies' power consumption classifies the load into several classes, design a bill payment model indicating the power consumed and penalty, identify the overload and the need for load in the network, and maximize the security of consumer privacy by performing hybrid encryption techniques. The SM based residential load management and privacy assurance are focused in this paper.

1.1. Related works

Authors in [17] have contributed to improving the demand response through algorithms by measuring the demand and controlling the load. Controlling of household appliances is achieved by an artificial neural network (ANN) for reducing energy consumption. The Active load, i.e., household appliances in a residency, was monitored and flexibly managed. Based on the household appliances, loads were categorized into two as controllable load and uncontrollable load. Load measurements are analyzed by an artificial neural network (ANN) operated by the trained data [18]. ANN uses a two-layer feed-forward along with back-propagation. The factors that are considered for training are minute-based real and reactive power. However, ANN performs faster it requires a set of data to be trained. Authors in [19] proposed to meet the demands of residential buildings incorporating an intelligent residential energy management system.. To monitor the load, they were broadly classified into three categories as non-interruptible and non-schedulable loads (NINSLs), interruptible and non-schedulable loads (INSLs), and schedulable loads (SLs). Warning messages are generated if the power consumption exceeds the limit. An external battery was operated to manage load, and the residency owner was not intimated regarding the load peaks.

To schedule residential loads, authors in [20] developed a demand response strategy. The residencies' loads were classified into noncontrollable load, interruptible load, adjustable load, and shiftable load. The local historical data were processed with the Copula function and Monte Carlo simulation. The load setting parameters are then defined based on every customer's comfort; however, it may cause electricity demand. Demand-side management in the residential sector was involved in investigating electricity tariffs and usage of household appliances. The daytime energy consumption and billing were not minimized since the peak loads were not measured and controlled. A two-phase distributed stochastic linear programming management based cooperation game algorithm was developed for payments and verifying the energy consumptions [21].

Also, an authenticated communication scheme was proposed for ensuring security in SM [22]. Here, a session key was generated while initializing the system, and a Merkle hash tree was constructed. The reports are

encrypted and compute a value and then transmit the message. The neighborhood gateway was responsible for authenticating the data received. The major problems exist in load management, billing strategies, and security. Detection of load states was executed using the k-means clustering algorithm to group the input signals and then use the k-Nearest Neighbor (k-NN) algorithm for the classification of load states [23]. The conventional procedure was followed for these methods, and the results of classification were based on the clustered data. According to the variation in an input signal, the clustering needs to be re-created for efficient classification, and the only limited number of clustered were created based on the k-value.

In [24], a low-cost universal smart energy meter (USEM) with demand-side load management was proposed in which the emergency load was previously stored in the utility server, based on which the load was managed in this system. The loads were categorized into two categories as heavy load and light load. If the consumer exceeds the permitted load, then an SMS will be sent from the control room to the user. On receiving this SMS, the heavy load must be switched off. In this case, the emergency load condition by a user could not satisfy demand since the electricity production failed to support all the residential customers.

Security in residential load management was presented in [25], [26]. The measured SM values were sent to another end, in which security was essential, and it was provided by the Unique String Authentication procedure. The Android-based application was created for enabling communication between the user and the utility center, in which the status is updated on the user's mobile. Neverthel

ess, if the user's mobile is theft, the status can be viewed by any third person. However, it was equipped with security; they are vulnerable to physical tampering, which tends to major in measured values. Overall, problems defined in this residential sector of load management and security are resolved with the proposed SRS-LM system solutions.

1.2. **Motivation and Research Contributions**

The major motivation of this research work is to design a load management system in smart grid in order to optimise the power consumption of the smart residencies. The anonymity of the consumers is preserved in order not to monitor the behavior activities of the consumer. The major issues encountered in this research area are mentioned below,

- Large scale network – the smart grid system is utilised by all the people making it vulnerable to load imbalance which is caused mainly due to uncertainties.
- Improper user anonymity management –user anonymity is a vital factor in designing the load management system. Monitoring of user load leads to gaining knowledge about user behaviour which further leads to criminal activities.

These issues are considered in order to design the secure load management system. The primary objectives of

this research work are,

- To monitor the power consumption of the smart residencies by classifying the load into several significant classes.
- To design a bill payment model indicating the power consumed and penalty.
- To identify the overload and the need for load in the network.
- To maximise the security of consumer privacy by performing hybrid encryption techniques.

The major contributions of this paper are enlisted below,

- A three-fold load management system for demand-response in residential homes integrating a Hopfield neural network for identifying load status from the residential sector and categorised into three classes as active load, affordable load, and inactive load; a novel fuzzy-logic based for electricity bill payment verification, and a Markov chain model to manage the power consumption and identity surplus usage of electricity.

- A combination of blowfish and ECC-based hybrid cryptography for secure accessing SMs measurements by consumers via IoT device. The data's decryption is applicable only when the device is present with the corresponding consumer since this work considers behavioral information. IoT devices are subjected to lesser computation and hence, only a partial key is stored, which also assists in ensuring security.

2. Proposed SRS-LM System

The proposed SRS-LM system is presented to envision and manage load in the residential sector and provide security for the SM measurements.

2.1. System model

SRS-LM system is comprised of IoT devices, load management system, residencies, and the utility grid. Each residency is deployed with multiple household appliances and an SM. SM plays a vital role in the SRS-LM system responsible for collecting electricity usage information from their residency. The designed SRS-LM system consists of N number of residencies as $R_1, R_2, R_3, \ldots\ldots, R_N$ with the corresponding number of SMs represented as $SM_1, SM_2, SM_3, \ldots\ldots, SM_N$ and IoT devices for each residency as $D_1, D_2, D_3, \ldots\ldots, D_N$. The major home appliances that are operated in residency are light, fan, microwave oven, personal computer, air conditioner, refrigerator, water heater, air cooler, water pumps, grinder, dishwasher, and clothes dryer. Household appliances are categorized into three, based on their requirements and energy consumption.

Household appliances in each residency are varied, and according to their utilization, the bill payment cost is updated. The household appliances are categorized into essential appliances, flexible appliances, and optional appliances, as shown in Table 1. These categories are split for identifying the load at a residency.

Table 1 SRS-LM Categorize of Appliances.

Category	Type	Household appliances
I	Essential appliances	Lamp, fan, microwave, oven, personal computer
II	Flexible appliances	Air conditioner, air cooler, water heater, refrigerator
III	Optional appliances	Water pump, grinder, dishwasher

Initially, three-fold load management is operated using readings from SMs. The three-process handled are Hopfield neural network for load classification, fuzzy logic for payment prediction, and Markov chain to identify residency states. Lastly, the SM measurements and load updating are accessed by the residency owner via an IoT device. The load classification is carried out using an artificial neural network as it provides high accuracy in classification, and it is not tough to gather a huge amount of smart meter reading for the training process. The measurements are stored in an encrypted format that is securely accessed only by the IoT user. A hybrid blowfish-ECC algorithm is used for secure data storage. IoT devices are supposed to have the issues as low-memory, low-power, and they are resource-constrained. Due to these limitations in IoT, the SRS-LM system minimizes operations in IoT devices and stores partial keys for security purposes.

SRS-LM system gathers data from SMs deployed in each residency and is processed in the load management system as depicted in Fig. 1. The load management is enabled to compute load status, and on the other hand, the bill settlement is also predicted.

2.2. Load management

Load management is comprised of three major processing as load category classification, load status prediction, and bill payment determination. Bill payment and load status prediction are simultaneously performed.

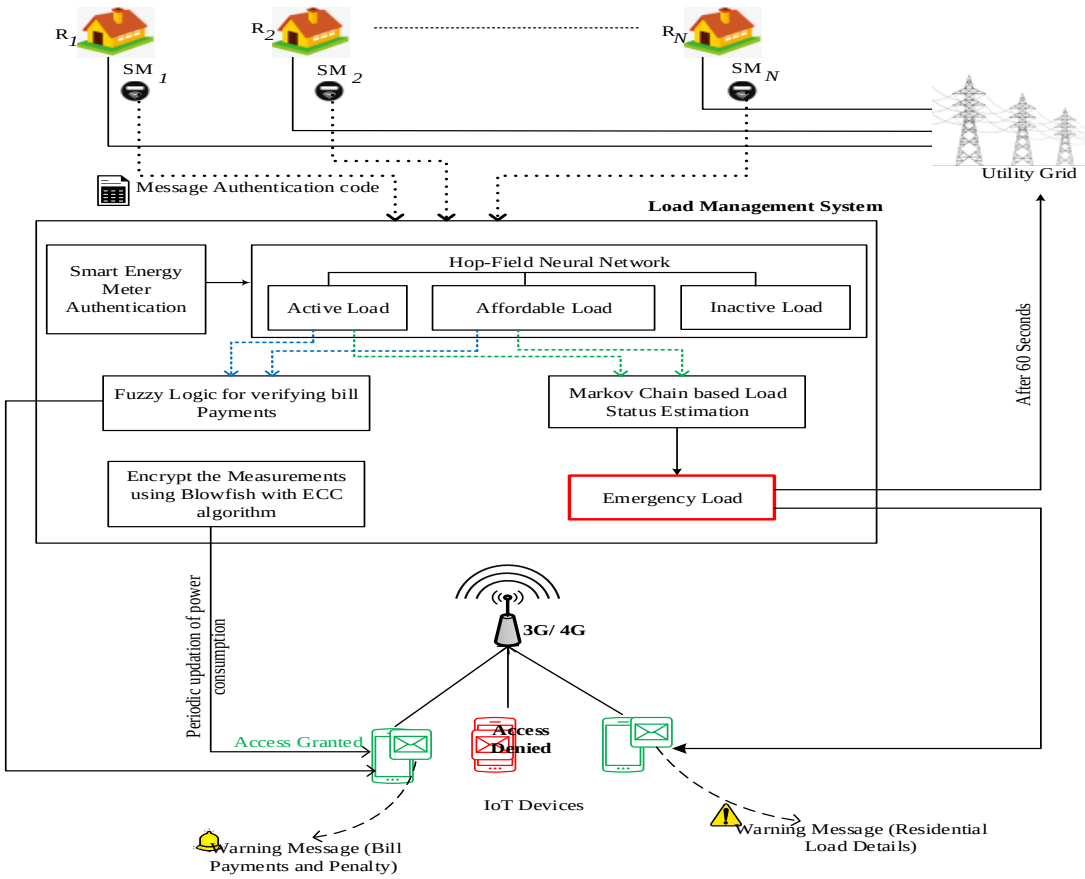

Fig. 1 Proposed SRS-LM system model.

The output from this system is updated, and in case of a warning message, they are intimated to the user's IoT device. This three-fold load management system is operated using Hopfield neural network, fuzzy logic, and Markov chain. The working of these three blocks for a peculiar process is detailed. The load management system initially authenticates the SM using its Identity (ID) and secret value (s_e). Using these two constraints, a message authentication code (MAC) is generated, and only after authentication of SM, the other load management process is performed. This MAC is dynamically generated during the submission of SM measurements. Let R_1 having SM_1 with S_{Id1} and s_{e1} as secret value. The MAC value is expressed as:

$$MAC_{SM} = S_{Id1} \oplus s_{e1} \qquad (1)$$

The generated MAC_{SM} is exchanged and verified, and then for submission of the next measurements, the MAC is supposed to be as follows:

$$MAC_{SM} = S_{Id1} \oplus (s_{e1} + 1) \quad (2)$$

This computation is simpler, so the SM determines it, and after completion of authentication, their measurements are analyzed by the load management system.

2.2.1.Hopfield Neural Network

Hopfield neural network is one of the types of ANN encompassed of nodes on a single layer. The nodes in Hopfield neural network are updated synchronously by clock time variations. The nodes participating here exist with connectivity based on the determined weight values between the connected nodes.

Hopfield neural network uses the measurements from SM as input and classifies the load into active, affordable, and inactive. The feedback loops formed in this network reflect its performance in enriching learning capability. This is efficient in solving complex computational problems. The household appliances used in three categories are depicted in the above section 4.1. The Hopfield neural network is designed with a single layer of nodes connected with other nodes as feedback connections, which helps redirect the output into the input. Here the number of nodes, inputs, and outputs are equal; in this SRS-LM system, the total number of residential as $R_1, R_2, R_3, \ldots\ldots, R_N$ nodes are constructed (see Fig. 2). The nodes are binary threshold nodes since they are served as a content addressable memory system. According to the arrival of input, it defines a corresponding weight value. The received input's weight value is determined from individual residential measurements formulated based on the node's weight connectivity and state. The weighted sum of the nodes I is estimated from the following expression:

$$I_i = \sum_{j=1}^{N} w_{ij} s_j \quad (3)$$

Where w_{ij} represents the connectivity weight exists between i and j, then s_j is the state of the node j. Training in Hopfield neural network is handled using learning rules, in SRS-LM a Storkey learning rule is applied for better error minimization. The mathematically defined Storkey learning rule is formulated as follows:

$$w_{ij}^{0} = 0 \quad \forall i, j \quad (4)$$

$$w_{ij}^{k} = w_{ij}^{k-1} + \frac{1}{N} \xi_i^k \xi_j^k - \frac{1}{N} \xi_i^k h_{ji}^k - \frac{1}{N} h_{ij}^k \xi_j^k \quad (5)$$

The above learning rules enable the properties of local and incremental for updating the connectivity weight information and increases if there is no need for information from any other previously trained pattern,

respectively. Herein (4) and (5), the w_{ij}^{k} is the weight estimated between i and j only after the k^{th} pattern is learned, ξ^{k} denotes the new learning pattern, and the local field h_{ij}^{k} is given as:

$$h_{ij}^{k} = \sum_{n=1, n\neq i, j}^{N} w_{in}^{k-1} \xi_{n}^{k} \qquad (6)$$

Hopfield neural network is designed to classify the loads based on the utilization of categories of household appliances. Figure 2 depicts the Hopfield network with a single layer for classifying the load, the inputs from the residencies are $\{x_1, x_2, x_3, \ldots x_i \ldots, x_N\}$, and the corresponding outputs are $\{y_1, y_2, y_3, \ldots y_i \ldots, y_N\}$. The inputs are received from each SMs that are deployed in the residencies $\{R_1, R_2, R_3, \ldots\ldots, R_N\}$. Output in Hopfield network is obtained for each residency in the determination of their current class.

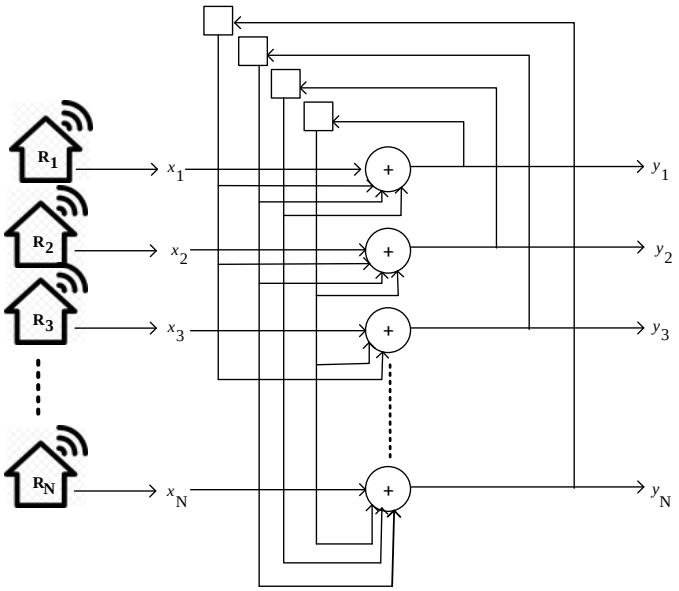

Fig. 2 Hopfield network in SRS-LM.

The significance of the Hopfield neural network is its use of associative memory. This memory is enabled to store part of the information using which the rest of the pattern is recollected. Recalling the previous patterns supports to have prior knowledge of load class for each residency. The load is categorized into three classes, as shown in Table 2.

Table 2 Hopfield neural network based on load classification.

Class	Load type	Condition
1	Active load	All category (I, II, and III) appliances are ON
2	Affordable load	Only appliances in category I and II are ON
3	Inactive load	All category (I, II, and III) appliances are OFF

The states of nodes in the proposed SRS-LM are estimated as:

$$S = \begin{pmatrix} s_1 & s_2 & \dots & s_i & \dots & s_N \end{pmatrix} \quad (7)$$

States s for each node are formulated in a matrix that is trained, and here the three classes are the possible states of the load. The state of the node s_i is determined as:

$$s_i = sign\left(I_i - Th_N\right) \quad (8)$$

Where Th_N denotes the threshold. Here, $sign(x) = 1 \forall X \geq 0$ and here, $sign(x) = -1 \forall X < 0.$ Then the weighted values for each node in the constructed Hopfield network are determined in a matrix, i.e., zero diagonal. As in this neural network, no node is connected to itself, it should obey $w = w$, and the weight of the node's connectivity is expressed as:

$$W = \begin{pmatrix} 0 & w_{12} & \dots & w_{1i} & \dots & w_{1N} \\ w_{21} & 0 & ,\dots & w_{2i} & \dots & w_{2N} \\ \vdots & \vdots & & \ddots & \vdots & \vdots \\ w_{i1} & w_{i2} & \dots & 0 & \dots & w_{iN} \\ \vdots & \vdots & & \dots & \vdots & \ddots \\ w_{N1} & w_{N2} & \dots & w_{Ni} & \dots & 0 \end{pmatrix} \quad (9)$$

The threshold Th_i is given for each node according to their household appliances that are present. So here, it is not necessary to have all the listed household appliances in each residency. Hence the threshold for nodes is given in the matrix format as:

$$Th_N = \begin{pmatrix} \theta_1 \\ \theta_2 \\ \vdots \\ \theta_i \\ \vdots \\ \theta_N \end{pmatrix} \qquad (10)$$

The terms $\{\theta_1, \theta_2, \ldots\ldots \theta_N\}$ are the individual threshold values for each node. Based on the presence of household appliances in each residency, the threshold is varied. If the user includes a new household appliance, then the threshold is also updated. After detecting the residential sector load classes, the utilization of the categorization of load at the residency is identified. Then, individual residential payment status is verified, and on the other hand, the exact utilization of load by the residency is predicted.

2.2.2.Markov chain

The prediction of the states of residency is carried out based on the predefined electricity utilization limit. The Markov chain analysis is deployed in this process as it possesses highly effective forecasting characteristics performed in cloud security on Information Technology applications [27], [28]. The transition probability is computed based on the load type and it is updated by using the equation (12).

In this SRS-LM load prediction, three load states are considered as $X_n = \{s_r, s_c, s_g\}$ i.e. normal state, critical state, and emergency state. Discrete time-based Markov chain, which deals with n transition time alternately. The Markov chain process determines the load state that can either stay in its previous state or move into another possible state. This Markov chain is also equipped to predict future states with respect to the present state. Let X_0 be the initial state in which the system currently exists.

The transferring probability of the system from one state to another is mathematically represented as:

$$P_{lm} = P_r\left(X_{(n+1)} = m \mid X_n = l\right), \ \forall n = 0,1,2,\ldots \qquad (11)$$

Where l and m are the probable states in the system, then the probability of state m after $n+1$ is given as:

$$P_{lm} = P_r(X_{(n+1)} = m \mid X_n = l, X_{(n-1)} = l-1, X_{(n-2)} = l-2 \ldots X_0), \forall n \geq 0, l, m, l-1\ldots \qquad (12)$$

The possible state transitions in the proposed SRS-LM predict the probability of state transition. The transition of any other states to normal state is provided by the sum of $P_{00} + P_{10} + P_{20}$, which their sum of probabilities is equal to 1 according to (13.a). This also applies for the other two states transitions; from any other state to critical state $P_{01} + P_{11} + P_{21}$ according to (13.b), and for the transition to emergency state $P_{02} + P_{12} + P_{22}$ according to (13.c), as seen in Fig. 3.

$$\sum_{i=0}^{2} P_{i,0} = 1 \qquad (13.a)$$

$$\sum_{i=0}^{2} P_{i,1} = 1 \qquad (13.b)$$

$$\sum_{i=0}^{2} P_{i,2} = 1 \qquad (13.c)$$

The transition matrix formulation of the states of Normal, Critical, and Emergency loads is defined in (14). Since, in a Markov chain, only the present state affects what is happening next, to have a transition between actual, whatever it is, and a following state, the sum of the set of probabilities is equal to one; that is, the probability of change to a specific state at a future time *t* depends only on the current state, and not in any previous state.

$$P_{|} = \begin{bmatrix} P_{0,0} & P_{0,1} & P_{0,2} \\ P_{1,0} & P_{1,1} & P_{1,2} \\ P_{2,0} & P_{2,1} & P_{2,2} \end{bmatrix} \qquad (14)$$

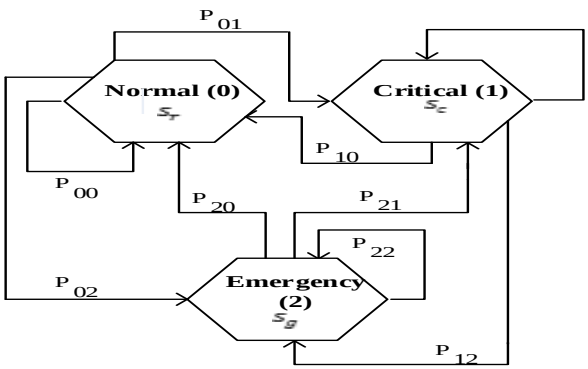

Fig. 3 Load status prediction using Markov chain.

Markov chain process predicts a sequence of possible events based on the probability of the events estimated. Each state is possible to change into another state and hence continuous building the Markov chain model. Three states compose the probabilities of state transition for every state. The normal state is $\{P_{00}, P_{01}, P_{02}\}$ where no state change can happen and move to a critical or emergency state Similarly, the other two states as critical and emergency are supposed to have the probabilities $\{P_{10}, P_{11}, P_{12}\}$ and $\{P_{20}, P_{21}, P_{22}\}$, based on the state transition, each residency's load status is predicted. If the load status is s_g, then the higher power consuming load in category II and III are insisted to turn it off. In turn, if the load status remains the same as before, then the utility grid is informed to shut down electricity to that residency. "The runtime overhead of the Markov chain to predict load category is denoted by $\otimes$ $(n. m)$ where

n is the number of iterations, and *m* length of model, i.e., input number, that is the number of devices and loads to be categorized. Hence, the algorithm was adjusted to 500 iterations as the maximum value with a length of the model changing as different iterationd occur. Since runtime of algorithms highly depends on code and hardware, algorithm efficiency is often evaluated in terms of Big-O notation that consider algorithm performance as data input increases, in this case Big-O notations takes a linear form of $O(m)$."

2.2.3.Fuzzy logic

In this section, the proposed SRS-LM system is presented to envision and manage load at the residential sector along with the provisioning of security for the SM measurements. The fuzzy logic is deployed for verifying bill payments as they have been vastly used as expert and control system providing decisions accurately in a fast manner [29], [30].

Electricity bill payment is one of the essential processes involved in detecting whether the individual residential owner has paid the bill. Also, we intimate the user to pay bill priory to avoid unnecessary penalties. Fuzzy logic considers the last electricity payment date and penalty value for modeling fuzzy rules. The fuzzy logic control system is flexible, and it allows observations from the input parameters.

The fuzzy rules are supposed to be binary sets comprised of two-valued logic as True / False. A fuzzy logic control system is designed with the functioning of four consecutive blocks as fuzzification, rule base, interference engines, and defuzzification. In SRS-LM, two inputs are considered and processed to retrieve an output whether the payment is completed or incomplete (see Table 3).

Table 3 Fuzzy rules.

Inputs		Fuzzy output (F_o)
Previous bill payment (PP)	Penalty (P)	
True	True	Paid
True	False	Paid
False	True	Paid
False	False	Bill not paid

- Fuzzy Block I (Fuzzification):

Fuzzification is the first block that receives input parameters and transforms it into operable values of degree of membership functions. Each linguistic term has its degree of membership for the corresponding input parameter,

which depicts the degree of belongingness of the member. The key processing in fuzzification is mapping the input parameter values involving predefined fuzzy membership functions. Linguistic variables are numerical values that define the scale based on membership functions. The membership function for triangular fuzzy model can be represented as,

$$\mu(C_i) = \begin{cases} 1 & , C_i = C_0 \\ 0, & otherwise \end{cases} \quad (15)$$

- Fuzzy Block II (Rule Base):

Rule base is the key block present in fuzzy logic system, which is deployed with the knowledge of building a set of rules. The rules are developed in the 'If-Then' format that mimics operators' logic as AND, OR, and NOT. From these Boolean logic operators, OR operator is used in SRS-LM system. The Takagi-Sugeno fuzzy model defines rules as:

Rule 1 – If $(PP = True \mid P_y = True)$, Then $F_o = 1$

Rule 2 – If $(PP = True \mid P_y = False)$, Then $F_o = 1$

Rule 3 – If $(PP = False \mid P_y = True)$, Then $F_0 = 1$

Rule 4 – If $(PP = False \mid P_y = False)$, Then $F_o = 0$

The true and false represents 1 and 0 respectively, the output F_O having 1 and 0 denotes bill paid customer and unpaid bill customer, respectively. | is the OR operator which is used to define fuzzy rules. The membership functions are modeled into triangular sets having equal widths. The rule states that if both the PP and Py is false, the output is detected as a bill not paid; otherwise, the output is presented as paid.

- Fuzzy Block III (Interference Engine):

The interference engine handles three steps as aggregation, activation, and accumulation. The aggregation is performed for estimating the degree of fulfillment (d_{ff}) for the defined f rules. Then activation is involved to mitigate the d_{ff} by determining a weighted factor $w_f \in [0,1]$. Using this, the d_{ff} is altered as follows:

$$d_{ff}^{*} = w_f * d_{ff} \quad (16)$$

Where d_{ff}^{*} is defined as a degree of confidence that is determined for adapting the defined rules under the considered input-output relationship. On reducing the d_{ff} for each rule, then accumulation is determined by summing up all the output. As a result, the rules are constructed with two inputs and single output variable.

- Fuzzy Block IV (Defuzzification):

The variables in this block are converted into crisp values for processing. The center of gravity method is presented in defuzzification. Finally, the crisp output F_o is mathematically estimated using the center of gravity as:

$$F_O = \frac{\sum_i \mu(c_i) c_i}{\sum_i \mu(c_i)} \qquad (17)$$

From this, c_i is the discrete point running and $\mu(c_i)$ is the membership value that is defined in the corresponding membership function.

Fuzzy logic having higher precision and efficiencies for estimating the customer's payment details at a faster rate. A set of four rules as 2^p i.e. $p = 2$ denotes the total number of input parameters, hence $2^2 = 4$. These two parameters are enough to verify the user's payment. If the output is false, then the residential customer will be receiving a warning message to pay the bill via their IoT device. This warning message will include the cost to be paid for the energy consumed from their residential household appliances used. Power consumption cost [31] is determined from the following formulation:

$$C(R_i^t) = \begin{cases} C_1^t \times R_i^t & if \quad R_s^t \le G_s^t \\ C_1^t \times R_i^t & if \quad R_s^t > G_i^t \;\&\; R_i^t \le p_i^t \\ C_1^t \times p_i^t + C_2^t \times (R_i^t - p_i^t)^2 & if \quad R_s^t > G_s^t \;\&\; R_i^t \le p_i^t \end{cases} \qquad (18)$$

$C\left(R_i^t\right)$ is the cost of i^{th} residency at time t that is estimated from total power consumption $G_s = G_s^1, G_s^2, \ldots, G_s^T$, where T is the time slot in a day, P_i^t is the power allocated for the particular customer i. The cost per customer is determined, and their payment amounts will be included in the message.

2.3. User security

The proposed SRS-LM offers user security by encrypting electricity readings using hybrid blowfish and ECC algorithms. IoT users are enabled to access their household electricity utilization and keep update with the increase in load. Monitoring of load is associated to minimize electricity cost. In hybrid blowfish and ECC, a random number is generated [32]. Here in this proposed SRS-LM system, the integrated blowfish uses ECC for the generation of that random number. The unique point from ECC is used as a random number.

Blowfish is a symmetric-key cryptography that splits the message into blocks and encrypts 64-bit block. Blowfish algorithm performs subkey generation and encryption/decryption. The key size differs between 32 bits to 448 bits. Here 18, 32-bit sub-keys are composed by using P-arrays. This array initializes 4-s boxes, and then P-arrays are XORed for generating sub-keys. Determine a random number from the ECC algorithm. Let the ECC curve equation be:

$$y^2 = x^3 + ax + b \tag{19}$$

Two points P_1 and P_2 are selected from ECC as a new random number which is said to be 64-bit. Combining both P_1 and P_2 convert them into binary form for random number generation. This number should exist with a minimum of five 1's in its least significant 16-bit. Based on the 1's position in the least significant bit, the function is operated in 16 rounds. The plain text is performed XOR operation with the generated random number, and then they are divided into two sub-divisions. The sub-divisions are swapped on each iteration until total iterations are reached. Lastly, the two divisions are recombined, and encryption is terminated.

The encrypted plain text is updated on the user side while accessing the user decrypts and views the original measurement status. Since the increased theft of mobile devices, only a partial key is stored in the device in the SRS-LM system. IF a customer requests to access the information from the SRS-LM system, he/she will be authenticated based on the behavioral information. This information includes typing speed, location, and others. Only after authentication, the partial key will be provided for decryption. In this SRS-LM system, security is ensured even in the case of lost IoT devices. If the device is lost, then the user can register with a new device into the SRS-LM system and receive partial keys to keep updated with the electricity utilization.

3. Experimental evaluation

3.1. Simulation Environment

A simulation environment is constructed using the parameters that are highlighted in Table 4. The simulation parameters are not limited to this. SRS-LM system is proposed with load prediction and security in the residential sector. The SRS-LM system model is developed in network simulator–3.26 (Ns-3) installed on Ubuntu 14.04

LTS operating system. The developed SRS-LM is executed using two commands: ' *sudo ./waf configure*' and '*sudo ./waf build*'.

Table 4 Simulation parameters.

Entities	Specifications
Simulation area	1000 x 1000 m
Number of SMs (Static)	25
Number of IoT devices (Dynamic)	25
Load management server	1
Number of measurement packets generated	50 – 100
Measurement time interval	5 – 7 seconds
Mobility model (IoT mobile device)	Random waypoint mobility model
Mobility speed	10 – 50 mps
Transmission rate	100 Mbps
Simulation time	300 seconds

This work was implemented in a simulation tool. We have properly specified individual residency with the above-discussed number of household appliances, and their appropriate power consumption values are fed into. Table 5 depicts the load and their load values that are used in the SRS-LM system.

Table 5 Load power consumption.

Category	ID	Load	Power rating / kW
I	01	Light (Fluorescent lamp)	0.04
	02	Fan	0.10
	03	Microwave oven	0.8
	04	Personal computer (charging)	0.05
II	05	Air conditioner	1.5
	06	Air cooler	1.0
	07	Water heater	2.0
	08	Refrigerator	2.4
III	09	Water pumps	2.3
	10	Grinder	0.5

From the load power of each household appliance, SM in individual residency delivers the values to the server. The server is fed with a three-fold load balancing with a hybrid cryptography algorithm. Using the parameters as shown in the above table, the simulation setup is generated as depicted in Fig. 4. According to the simulation setup, the proposed SRS-LM system's results are obtained and compared with previous USEM.

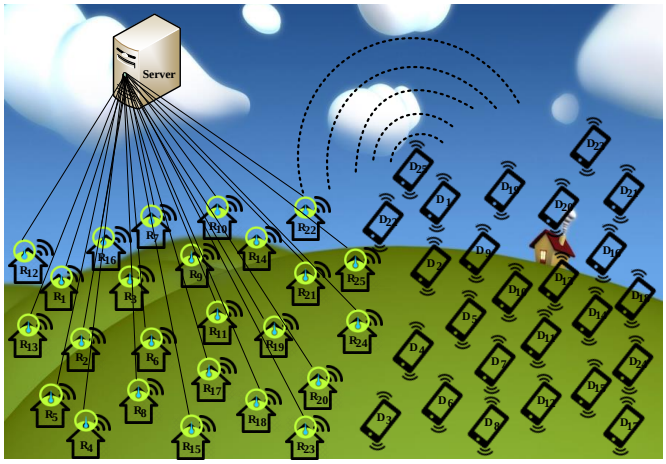

Fig. 4 Ns-3 SRS-LM simulation setup.

3.2. Comparative results

The proposed SRS-LM system procedure is compared with USEM, and the performance efficiencies are discussed. In USEM, the load management system emergency load was determined from the user-defined load condition. However, it works well for a single residency it tends to cause improper management among a residential sector. The performance is evaluated in terms of the following metrics: load power, peak load reduction, power cost, power utilization, and computational time.

3.2.1.Load power

Load power is defined as the power consumed by different household appliances at residency. The load power is variable in accordance with the presence of appliances in residency.

According to the increasing number of residencies, power increases due to the use of all household appliances. Figure 5 demonstrates the performance of load power by comparing the proposed SRS-LM with USEM. In USEM, a single residency consumes 0 – 80kW, whereas our proposed work SRS-LM deals with 25 residencies, and the load power is a little higher than the previous work. As per the increase in execution time, the number of residencies operation is increased, and hence the load is gradually increased, but the prediction of accurate load

status manages load at the residential sector with 25 residencies. The variation in minimum to maximum power for each household appliance is involved in load power estimation.

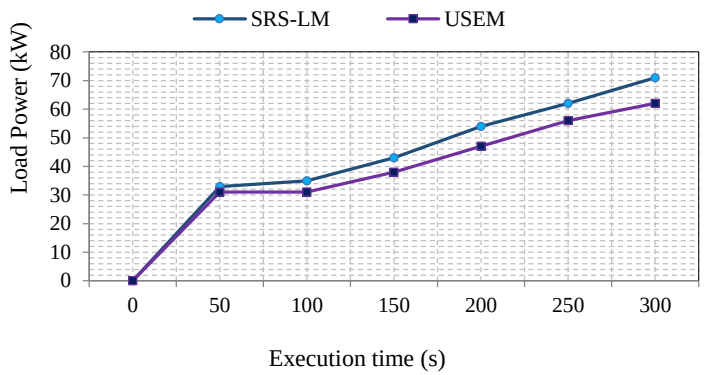

Fig. 5 Comparative results for load power.

3.2.2. Peak load reduction

Peak load reduction is present to manage the load when it exceeds the limit. The minimization in peak load reflects on the reduction in the power cost of each consumer. Peak load reduction requires accurate load prediction.

In SRS-LM, peak load is predicted from the Markov chain, which initially identifies the load category in which that residency is activated currently. Figure 6 depicts the comparison of peak load reduction of proposed and existing USEM.

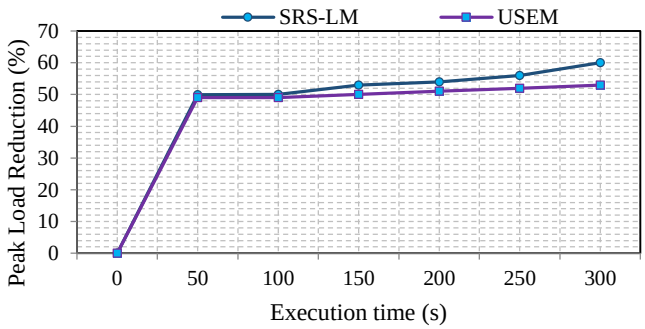

Fig. 6 Comparative results for minimization of peak load.

In SRS-LM, more than 40% of peak load is reduced with an increase in the execution time. This is possible as the proposed SRS-LM performs classification of load and accurate prediction of load, resulting in increased load reduction. Comparatively, USEM possesses lower load reduction due to a lack of effective load management.

Peak load reduction for 25 residencies greatly impacts minimizing power cost for all the consumers, and the dynamic management of emergency loads is a potential benefit for consumers.

3.2.3.Power cost

Power cost is a significant metric that estimates the price for the utilized electricity power. Increasing electricity usage and ignoring peak load reduction will certainly lead to higher power costs. Power cost is estimated from the above sections using the formulated equation (18). Detecting peak load in SRS-LM and USEM is designed to minimize the power cost of the consumer. Power cost for residency is varied timely based on the use of different household appliances.

Figure 7 shows comparison results of SRS-LM and USEM based on their power cost. When the execution time reaches 300s, all 25 residencies are active state using a certain load, whereas in USEM, a single residency is present entirely. Power cost is an increasing factor that gradually increases in peak times, and it has eventual reduction while managing loads efficiently. Power cost is estimated in terms of kW, i.e., electricity use.

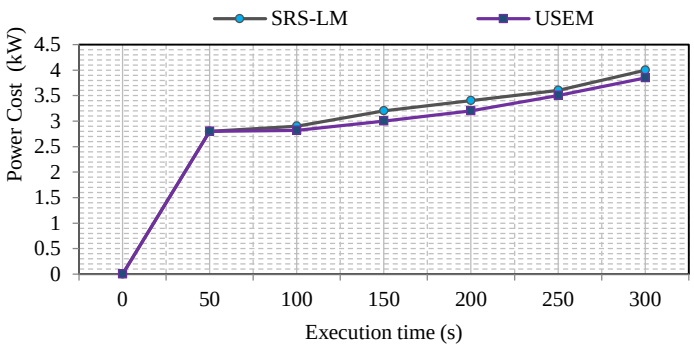

Fig. 7 Comparative results for power cost.

3.2.4.Power utilization

Power utilization is analyzed in terms of power usage and total power consumption in the deployed environment. In Table 6, the power usage with respect to the number of residency and power consumption is given with respect to execution time.

Table 6 Power utilisation.

Number of residencies	Power usage (kW)		Execution time (s)	Total power consumption (kW)	
	SRS-LM	USEM		SRS-LM	USEM

5	11	12	100	41	42
10	14	15	150	42	43
15	19	21	200	43	45
20	28	30	250	45	48
25	41	45	300	50	52

The existing USEM is presented for more than one residence, which resulted in higher utilization of power than the SRS-LM. However, only a smaller variation in power utilization, it impacts the changes in total power consumption. Minimizing the total power consumption by balancing the load is the key goal of SRS-LM. Monitoring SM measurements and predicting the load obtains moderate power consumption.

3.2.5. Computational time

Load in individual residency is predicted using three-fold load balancing, which deals with certain mathematical computations to identify the load and update customers through their IoT device. Computation time is determined for predicting the load status of the residency.

Computational time is plotted concerning the number of increasing residencies as depicted in Fig. 8. Computation time gradually increases with the growth of the number of residencies, since additional involvement of residency includes processing of household appliances. This comparison shows that the computation time for the proposed SRS-LM decreases while USEM has a higher time to predict load status.

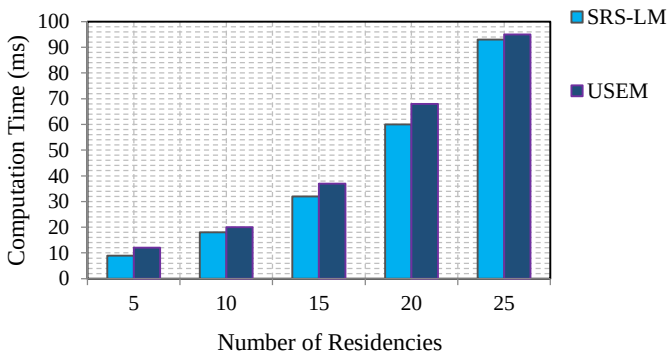

Fig. 8 Comparative results for computational time.

The Hopfield neural network and Markov chain in SRS-LM guarantees lesser time for computations to predict load accurately. While in the previous USEM, the load is predicted based on user-defined threshold values. The owner's load preference is not advisable since it creates electricity scarcity problems, and different limits by each residency become complex and consume time for load prediction.

3.3. Security analysis

Security is majorly focused in this paper by presenting a hybrid algorithm that integrates blowfish with the ECC algorithm. The measured values from SMs are securely accessed by consumers using their IoT devices. Initially, the originality of SM is verified by generating MAC; later, the data are encrypted using a hybrid algorithm and stored.

The stored information is periodically updated according to the changes in power consumption. This information is accessed from anywhere by the user. Table 7 illustrates the execution time of the blowfish ECC algorithm, whose data size is 1 KB. Here the SM measurements are numerical values of power readings, and those data are smaller in size. The performance of the blowfish ECC algorithm in SRS-LM is evaluated in terms of authentication, confidentiality, and data integrity. The three constraints of security analysis are discussed below.

Table 7 Execution time for the hybrid algorithm

Number of rounds	Execution time (s)
4	0.08
8	0.09
12	0.12
16	0.14

3.3.1. Authentication

In the proposed SRS-LM, the communication is authentic since the behavior of the user is determined. Behavior is based on the details of built-in sensors that are extracted. Here, it is impossible for a third person to access SM data since only a partial key is present in IoT devices. Also, it gives the SM data only after authenticating the user based on their behavior.

3.3.2. Confidentiality

This constraint is also attained in the SRS-LM system, which stores the data after encrypting it. Encrypting the SM measurements and load status information using a hybrid blowfish ECC algorithm enables to provide

confidentiality since no one can read this information unless the corresponding user is authenticated and decrypt the information.

3.3.3. Integrity

The SM values in SRS-LM are encrypted, and so it cannot be altered by any third party. The communication between IoT and server is handled in a secure channel. Also, the users are authenticated before receiving the information, which ensures data integrity.

The proposed SRS-LM system is accomplished with the goal of load management and security. Load management is attained by a three-fold process of load category detection, load status prediction, and bill payments verification. On the other hand, security is provisioned by authenticating SM, authenticating IoT devices, and hybrid cryptography-based secure data access. Also, to minimize computations and memory limitations in IoT devices partial key is stored, which supports security even if the device is stolen.

4. Conclusions

In this work, an SRS-LM system is developed for load management in the residential sector with the provisioning of secure access by customers using IoT devices. The readings from SMs are authenticated with MAC, and then based on the measurements, they are categorized into different loads. Three-fold load management is presented by designing Hopfield neural network, Markov chain, and fuzzy logic. Hopfield neural network classifies the load into three categories as active load, affordable load, and inactive load. Furthermore, the Markov chain is involved to predict the current load status as normal, critical, or emergency. This load status is enabled to give a warning message to turn off excessively used load at the residency. SRS-LM ensures secure accessing of SM measurements and load status by the applied hybrid cryptography algorithm. Blowfish algorithm is integrated with the ECC algorithm. Blowfish procedure is followed in which the random number generation is undergone by ECC. The comparative results for power utilization, load power, peak load reduction, power cost, and computation time have proven its better efficiency than the previous USEM system. In the future, it is planned to concentrate on a demand-side load management system.

CRediT author statement

Cristian Chiñas: Methodology, Software, Writing – Original draft preparation. **Jesus Aguila:** Investigation, Data curation. **Carlos Vargas:** Writing – Reviewing and Editing, Project administration, Validation. **Edith Garcia:** Supervision, Funding acquisition. **Julian Sotelo:** Conceptualization. **Elias Hurtado:** Visualization.

Competing Interests

There is no potential competing interests in this paper. All the authors have seen the manuscript and approved to submit to your jounal. We confirm that the content of the manuscript has not been published or submitted for publication elsewhere.

Acknowledgments

This work was Supported by National Council of Science and Technology (CONACYT) through the Ph.D. scholarship 705018. The authors would like to thank the University of Guadalajara, Mexico, and the Polytechnic University of Valencia, Spain, for all the collaboration and realization of this paper.

References

[1] K. Hopf, M. Sodenkamp, and T. Staake, "Enhancing energy efficiency in the residential sector with smart meter data analytics," *Electron. Mark.*, vol. 28, no. 4, pp. 453–473, 2018.

[2] A. Safdarian, M. Fotuhi-Firuzabad, and M. Lehtonen, "Optimal Residential Load Management in Smart Grids: A Decentralized Framework," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1836–1845, 2016.

[3] P. U. B. Albuquerque, D. K. d. A. Ohi, N. S. Pereira, B. de A. Prata, and G. C. Barroso, "Proposed Architecture for Energy Efficiency and Comfort Optimization in Smart Homes: Smart Home Architecture for Energy Efficiency," *J. Control. Autom. Electr. Syst.*, vol. 29, no. 6, pp. 718–730, 2018.

[4] M. Rastegar, M. Fotuhi-Firuzabad, and M. Moeini-Aghtai, "Developing a two-level framework for residential energy management," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1707–1717, 2018.

[5] T. Alquthami and A. P. S. Meliopoulos, "Smart House Management and Control Without Customer Inconvenience," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2553–2562, 2018.

[6] M. Hupez, Z. De Grève, and F. Vallée, "Cooperative demand-side management scenario for the low-voltage network in liberalised electricity markets," *IET Gener. Transm. Distrib.*, vol. 12, no. 22, pp. 5990–5999, 2018.

[7] V. J. Gutierrez-Martinez, C. A. Moreno-Bautista, J. M. Lozano-Garcia, A. Pizano-Martinez, E. A. Zamora-Cardenas, and M. A. Gomez-Martinez, "A heuristic home electric energy management system considering renewable energy availability," *Energies*, vol. 12, no. 4, 2019.

[8] J. Aguila-Leon, C. Chiñas-Palacios, C. Vargas-Salgado, E. Hurtado-Perez, and E. X. M. Garcia, "Particle swarm optimization, genetic Algorithm and grey Wolf optimizer algorithms performance comparative for a DC-DC boost converter PID controller," *Adv. Sci. Technol. Eng. Syst.*, vol. 6, no. 1, pp. 619–625, 2021.

[9] M. Li, G.-Y. Li, H.-R. Chen, and C.-W. Jiang, "QoE-Aware Smart Home Energy Management Considering Renewables and Electric Vehicles," *Energies*, vol. 11, no. 9, p. 2304, 2018.

[10] A. Agarkar and H. Agrawal, "A review and vision on authentication and privacy preservation schemes in smart grid network," *Secur. Priv.*, vol. 2, no. 2, p. e62, 2019.

[11] F. Knirsch, G. Eibl, and D. Engel, "Multi-resolution privacy-enhancing technologies for smart metering," *Eurasip J. Inf. Secur.*, vol. 2017, no. 1, 2017.

[12] Z. Guan, Y. Zhang, L. Zhu, L. Wu, and S. Yu, "EFFECT: an efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid," *Sci. China Inf. Sci.*, vol. 62, no. 3, pp. 1–14, 2019.

[13] C. Y. Acevedo-Arenas *et al.*, "MPC for optimal dispatch of an AC-linked hybrid PV/wind/biomass/H2 system incorporating demand response," *Energy Convers. Manag.*, vol. 186, no. February, pp. 241–257, 2019.

[14] J. Aguila-Leon, C. Chiñas-Palacios, E. X. M. Garcia, and C. Vargas-Salgado, "A multimicrogrid energy management model implementing an evolutionary game-theoretic approach," *Int. Trans. Electr. Energy Syst.*, vol. 30, no. 11, pp. 1–19, 2020.

[15] C. Vargas-Salgado, J. Aguila-Leon, C. Chiñas-Palacios, and E. Hurtado-Perez, "Low-cost web-based Supervisory Control and Data Acquisition system for a microgrid testbed: A case study in design and implementation for academic and research applications," *Heliyon*, vol. 5, no. 9, Sep. 2019.

[16] J. Ni, K. Zhang, X. Lin, and X. Shen, "Balancing security and efficiency for smart metering against misbehaving collectors," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1225–1236, 2019.

[17] J. Ponocko and J. V. Milanovic, "Smart meter-driven estimation of residential load flexibility," *CIRED - Open Access Proc. J.*, vol. 2017, no. 1, pp. 1993–1997, 2017.

[18] C. Chiñas-Palacios, C. Vargas-Salgado, J. Aguila-Leon, and E. Hurtado-Pérez, "A cascade hybrid PSO feed-forward neural network model of a biomass gasification plant for covering the energy demand in an AC microgrid," *Energy Convers. Manag.*, vol. 232, no. January, 2021.

[19] S. L. Arun and M. P. Selvan, "Intelligent Residential Energy Management System for Dynamic Demand Response in Smart Buildings," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1329–1340, 2018.

[20] S. Nan, M. Zhou, G. Li, and Y. Xia, "Optimal Scheduling Approach on Smart Residential Community Considering Residential Load Uncertainties," *J. Electr. Eng. Technol.*, vol. 14, no. 2, pp. 613–625, 2019.

[21] H. Qin, Z. Wu, and M. Wang, “Demand-side management for smart grid networks using stochastic linear programming game,” *Neural Comput. Appl.*, vol. 4, 2018.

[22] D. Abbasinezhad-Mood and M. Nikooghadam, “Efficient design and hardware implementation of a secure communication scheme for smart grid,” *Int. J. Commun. Syst.*, vol. 31, no. 10, pp. 1–16, 2018.

[23] Y. T. Quek, W. L. Woo, and T. Logenthiran, “Smart Sensing of Loads in an Extra Low Voltage DC Pico-Grid Using Machine Learning Techniques,” *IEEE Sens. J.*, vol. 17, no. 23, pp. 7775–7783, 2017.

[24] L. Labib, M. Billah, G. M. Sultan Mahmud Rana, M. N. Sadat, M. G. Kibria, and M. R. Islam, “Design and implementation of low-cost universal smart energy meter with demand side load management,” *IET Gener. Transm. Distrib.*, vol. 11, no. 16, pp. 3938–3945, 2017.

[25] P. Ganguly, M. Nasipuri, and S. Dutta, “A Novel Approach for Detecting and Mitigating the Energy Theft Issues in the Smart Metering Infrastructure,” *Technol. Econ. Smart Grids Sustain. Energy*, vol. 3, no. 1, 2018.

[26] N. S. Srivatchan and P. Rangarajan, “A novel low-cost smart energy meter based on IoT for developing countries’ micro grids,” *Concurr. Comput.* , no. September, pp. 1–10, 2018.

[27] M. H. R. Al-Shaikhly, H. M. El-Bakry, and A. A. Saleh, “Cloud Security Using Markov Chain and Genetic Algorithm,” *I.J. Electron. Inf. Eng.*, vol. 8, no. 2, pp. 96–106, 2018.

[28] M. Yang, R. Jiang, T. Gao, W. Xie, and J. Wang, “Research on Cloud Computing Security Risk Assessment Based on Information Entropy and Markov Chain,” *Int. J. Netw. Secur.*, vol. 20, no. 4, pp. 664–673, 2018.

[29] M. Alali, A. Almogren, M. M. Hassan, I. A. L. Rassan, and M. Z. A. Bhuiyan, “Improving risk assessment model of cyber security using fuzzy logic inference system,” *Comput. Secur.*, vol. 74, pp. 323–339, 2018.

[30] C. Sureshkumar and S. Sabena, “Fuzzy-Based Secure Authentication and Clustering Algorithm for Improving the Energy Efficiency in Wireless Sensor Networks,” *Wirel. Pers. Commun.*, vol. 112, no. 3, pp. 1517–1536, 2020.

[31] M. H. Yaghmaee, M. Samadi Kouhi, A. Saeedi, and M. Zabihi, “Demand side management controlling with personalised pricing method,” *CIRED - Open Access Proc. J.*, vol. 2017, no. 1, pp. 2666–2669, 2017.

[32] P. Patel, R. Patel, and N. Patel, “Integrated ECC and Blowfish for Smartphone Security,” *Phys. Procedia*, vol. 78, no. December 2015, pp. 210–216, 2016.