# PREVENTION OF ELECTRICITY THEFT IN A SMART UTILITY NETWORK USING RULE BASED APPROACH

**[1]Engr.O. Egonwa., [2]Prof. Eke James, [3]E. Kenekayoro, [4]Engr. E.A. Ahmed, [5]Engr. Emmanuel Okekenwa**

[1,3,4,5] Department of Electrical Electronics Engineering; School of Engineering Technology; Akanu Ibiam Federal Polytechnic Unwana,Afiko Ebonyi State. [2] Department of Electrical Electronics Engineering; Faculty of Engineering; Enugu State University of Science and Technology, Enugu State, Nigeria.

**DOI**: https://doi.org/10.56293/IJASR.2024.6105

**IJASR 2024**
**VOLUME 7**
**ISSUE 5 SEPTEMBER - OCTOBER** **ISSN: 2581-7876**

**Abstract:** This work puts out a proactive plan for stopping electricity thefts. A cyber security layer based on a unique Monkey-Banana Deceptive Algorithm (MBDA) for intrusion detection is used to reach the prevention phase. This algorithm was created by first presenting each stage to scenarios and then formulating a probability assignment model. It is based on the well-known 5 or 8-monkey theory. After that, the algorithm for detecting intrusion in the SEMs communication gateway is developed using MBDA probability assignment. Selected power theft-related indicators are then modelled to strengthen the prevention phase by creating a set of criteria to estimate the level of security risk. The MBDA was implemented using a self-generated assault, and the level of prevention is determined by the FIS model's output. Based on the conditions of the monitored metrics, the anomaly and confirmation models are applied to justify real fraudulent consumers. Implementing this proactive plan will improve real-time SEM protection, reduce reliance on energy consumption data analytics, lower false positive rates, do away with the practice of bogus financial sanctions, and greatly reduce the need for labour-intensive on-site customer-to-customer inspections, saving time, money, and stress by 95%. In a smart utility network, this proposed strategy is an effective deployment for the detection and prevention of electricity theft.

**Keywords:** Prevention, Detection, Smart Grid, Utility, Monkey Banana Deceptive Algorithm, Smart Electricity Meter, Cyber-Physical System.

## 1. Introduction

One of the basic ways of measuring the socio-economic development and growth of any country like Nigeria is the consumption of Electrical Energy, As the growth and development of the nation increases so also does the consumption of Electrical Energy. As the demand of electricity increases the need for effective distribution and accountability of energy consumption is essential for sustenance of the desired growth of the nation. The dynamics of achieving this sustainability is examined using the present power delivering schemes, planning and execution that brought about the use of Smart Grid (SG). The Smart Grid helps in effective power delivery by enhancing security of the network, resiliency, efficiency, flexibility and control of operations (Borlase, 2016; Clastres, 2011; Farhangi 2009; Kabalei and Kabalei, 2019). The effective implementation of Smart Grids (SG) depends heavily on energy efficiency, with Smart Electricity Meters (SEM) serving as a primary component of the Advanced Metering Infrastructure (AMI). Like every other Cyber-Physical System (CPS), it is vulnerable to cyber-attacks, and one common goal of these attacks is to steal electricity. However, SEM provides sufficient data that can be used to draw conclusions using analysis.

SEM (Smart Electricity Meter) is developed using (AMI) Advanced Metering Infrastructure to provide supporting communication and control for effective energy management is a major aspect of the Smart Grid (SG) ( Abushnaf et al, 2016; Mclaughlin et al, 2009). SG allows the flexibility of power consumption, pricing and control by using smart electricity meter (SEM) at both the customers and the substation, this is to enable easy communication between the SEM and utilities. This two way communication allows consumers to better control their energy usage.

## 2. Methodology

As shown in Figure 1, the proactive system for preventing energy theft is addressed with each stage addressing the process to achieve the set goals.

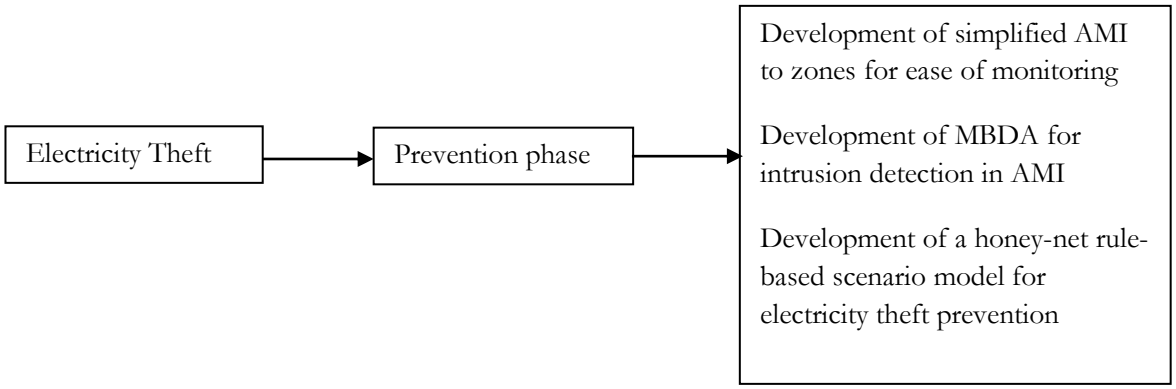


**Figure 1: Block Diagram**

The creation of a simplified AMI divided into zones to facilitate monitoring marks the beginning of the preventative phase. A rule-based scenario model using a fuzzy inference system (FIS) based on defined status of chosen parameters is presented after intrusion monitoring using a unique detection technique.

### 2.1. Simplified AMI Development into Zones

The protection zones are based on variety of parameters, including but not limited to:

1. Customer count in the area under investigation.
2. Customers' load consumption levels and consumer types.
3. Intuitive estimation of the customers' integrity (based on previous electricity theft records).
4. Average reported cases of energy theft.
5. Easy of identification customers, etc.

Figure 2, shows a specific neighbourhood network that is divided into protection zones (Zone 1, Zone 2, Zone 3, and Zone n) that each has n consumers depending on the aforementioned considerations. It is much simpler to monitor the data that is been collected from each zone. Monitoring of client consumption data, control measures and management of dynamic pricing information, are all made possible through the use of AMI, which links and shares this information with the utilities, consumers and third parties. Figure 3 shows the architecture for suggested monitoring system in protected area

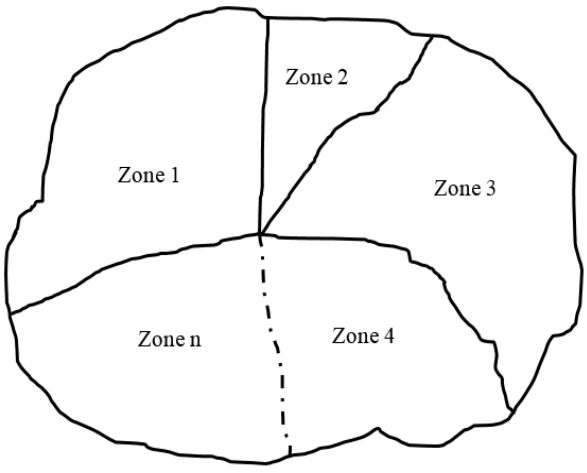


**Figure 2: Representation of protective zone for monitored SEMs in an area.**

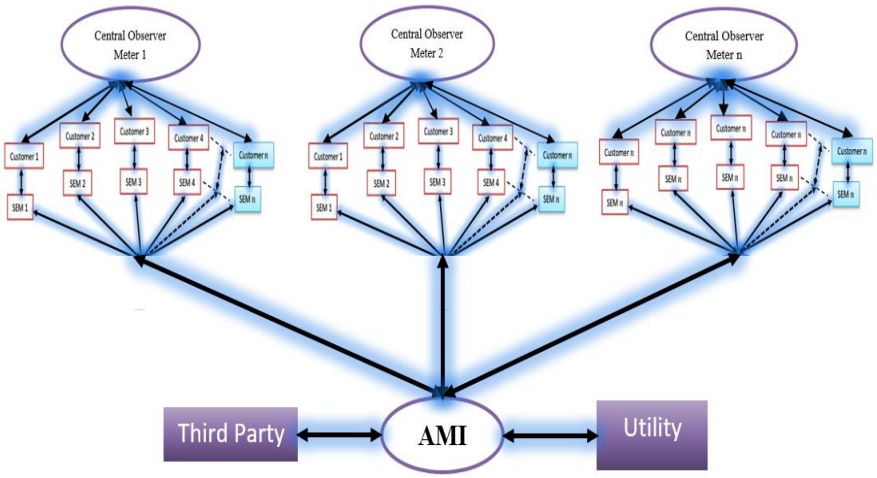


**Figure 3: Architecture of the proposed monitoring schemes for a set of zones in an area.**

### 2.2. Selection of Indicative Parameters for Electricity Thefts

Key network parameters from all the SEMs are chosen and modelled in each of the zones shown in Figure 2 to look for potential intrusions. To efficiently monitor and stop electricity thefts, these factors are simulated based on predetermined rules. Here are the chosen parameters (1) Communications Gateway C&C intrusion (2) False or aberrant patterns of consumption (3) The data on energy use has a false signature. (4) Untrue pricing (5) Time stamps (6) False invoices (or billing errors) (7) Status of the central observer meter

### 2.3. MBDA Mathematical Formulation

The mathematical formulas as follows to create the algorithm:

1) (Initialization): Set the C&C parameters that could serve as a honeynet for future intruders. Assign probabilities to the honeynet elements and take notice that they are currently scripts, just like the bots, but are prevented from causing harm to the system and are closely monitored based on the assigned probabilities.
2) Without any intrusion and assuming C&C parameters are the same in the set, the probability of any of the elements of H is set to $\frac{1}{n}$. Considering that any combination of the elements of H can carry out an attack, then, the intrusion monitoring probabilities of all possible combinations of the elements of H is $\left\{\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots .1\right\}$. The primary security is designed to block attacks from these elements and store their assigned probabilities as the base for detecting new elements. At this instant, there is no suspected intrusion because these probabilities, as assigned to the occurrences of the C&C parameters, are seen normal by the IDS since it is the base used to detect anomalies.
3) If any of the C&C parameters is removed or leaves the network, then, the number of elements in H is reduced to $n-1$ such that the intrusion monitoring probability for any of the remaining elements (for all combinations) will be $\left\{\frac{1}{n-1}, \frac{2}{n-1}, \frac{3}{n-1}, \ldots 1\right\}$. Updating the new length, $n = n-1$ then the intrusion monitoring probabilities for all possible combinations of the elements simply becomes $\left\{\frac{1}{n}, \frac{2}{\backslash}, \frac{3}{n}, \ldots 1\right\}$ again although with a different value of $n$.
4) If a new attack is launched (added to the initial data) to the C&C element, then, is updated and the probability detected by the IDS on these new elements are those strange to those of the honeynet set and the database will equally be updated to contain these new C&C parameters for subsequent monitoring but with probability of each element updated as well. Later, compromised elements are those probabilities not of the newly updated defence elements. However, for every addition, the number of honeynet elements is aggregated to a new value of $n = n+1$. The honeynet elements are each time assigned $\left\{\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots 1\right\}$ for all combinations.
5) If a number of the first original elements replaces any of the existing element(s) of H, then, the number of elements in the honeynet defense set becomes $n$ and the assigned probability on the elements remain $\left\{\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots 1\right\}$ for all combinations.

6) If a number of second original attack is launched to replace any of the old elements of the C&C, then, the number of elements in the defense remains $n$ while subsequent monitoring probability also remain $\left\{\frac{1}{n}, \frac{2}{\langle}, \frac{3}{n}, \ldots 1\right\}$ for all combinations. This is one advantage of the proposed MBDA as it doesn't have to learn the behavior of the attack to detect them at any time.
7) If cases v and vi continue in similar fashion, eventually all the $n$ attackers would be completely replaced. Assume the new set of elements are $H = \{b(i)\}$ but still with $n$ elements since they were simply replaced. The monitoring probabilities dynamically take the form $\left\{\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots 1\right\}$ for all combinations.
8) In all cases, intrusions are found to be of those elements whose probabilities are below the set threshold from the set of combinational probabilities.

### 2.4. Developed MBDA Algorithm

The mathematical formulations given in section 2.3 are transformed to the proposed MBDA Algorithm as given thus:

Step 1). (Initialization): Let the number honeynet set, H be $n$ and $H = \{a(i)\}$ for $i = 1,2,3,..n$ where $i \in Z^+$, then, the probability assigned to any of the individual element, $P[a(i)] = \frac{1}{n}; \frac{2}{n}$ ; for any two combinations and so on. Let $P_1, P_2 \ldots .. P_n$ represent the probabilities for all possible combinations of elements in H, and contained in a set $C$ , then, $C = \{P_1, P_2 \ldots .. P_n\}$ . Then, set the lowest value in $C$ to be the threshold, $P_0$ .

**Step 1** Step 2). For all possible combinations of the assigned probabilities, $C = \{P_1, P_2 \ldots .. P_n\}$. to the existing honeynet set, set threshold probability, $P_0$ and then assign probability to every newly found element. Note that if $P_0$ is $\frac{1}{n}$ , assigned probability to every other element is $\frac{1}{n+1}$, $\frac{1}{n+2}$, $\frac{1}{n+3}$ etc. Check for the presence of intrusion after every set period based on scenarios iii, iv, v and vi of the mathematical formulations as contained in Section 3.4.3.2. If one of the elements of $H$ is removed, then $= \{a(1), a(2), a(3) \ldots a(n-1)\}$ and $n$ is then updated to $n = n - 1$, then, Step 6.

**Step 2** If any new element, say, $b(j)$ is added to $H$, then, $H = \{a_1, a_2, a_3, \ldots, a_n, b_1, b_2, \ldots, b_m\}$. For all $a(i)$, $b(j) \in H$, for $i = 1, 2, \ldots, n$ and $j = 1,2, \ldots, m$ where $i, j \in \mathbb{Z}^+$, then $n = n + n(b(j))$ and $H$ is updated to $\{a_1, a_2, a_3, \ldots, a_n\}$, then, Step 6.

**Step 3** If a second original attack, say $d(j)$, is launched, then, for all $a(i)$, d(j) $\in H$, then for $i = 1, 2, \ldots, n$ and $j = 1,2, \ldots, m$ where $i, j \in \mathbb{Z}^+$ then $n = n + n(q(i))$, and $H$ is equally updated to $\{a_1, a_2, a_3, \ldots, a_n\}$, then, Step 6.

**Step 4** For all elements of $H$, determine $p(a(i))$ and If $\mathrm{P}(a(i)) \in \mathrm{C}$, output "No Intrusion detected" Else return "Intrusion detected" and return $a(i)$ as intrusion and activate the base security to block the threat, then update $H$ to include $a(i)$.

**Step 5** For all scenarios, Check if n($H$) $\geq N$, if Yes, shift n($H$) by removing the old $\frac{n}{2}$ elements and update $n = n - \left(\frac{n}{2}\right)$. Then, calculate new values for $\mathrm{P}(a(i))$.

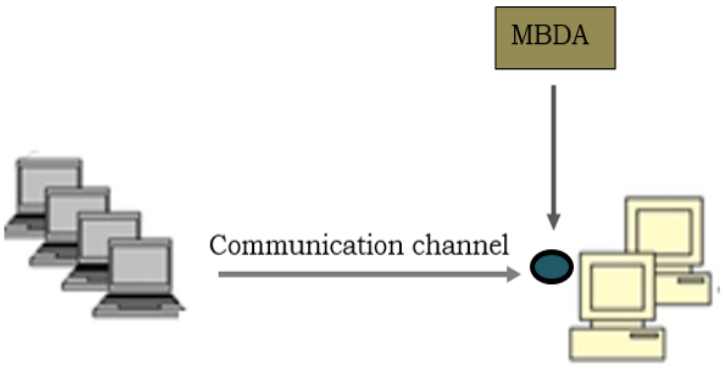


**Figure 4: MBDA Operation Spot**

The location of MBDA's activity at the communication gateway is shown in figure 4. This indicates that security is offered before information is shared. The capacity of the proposed MBDA to consistently detect approaching intrusion by assigning intelligent calculated threshold probabilities based on predetermined scenarios set it apart from conventional honeynets and other anomaly detection techniques. This probability distribution is uniformly distributed across all conceivable scenarios and depends on the number of traps (honeynet) elements.

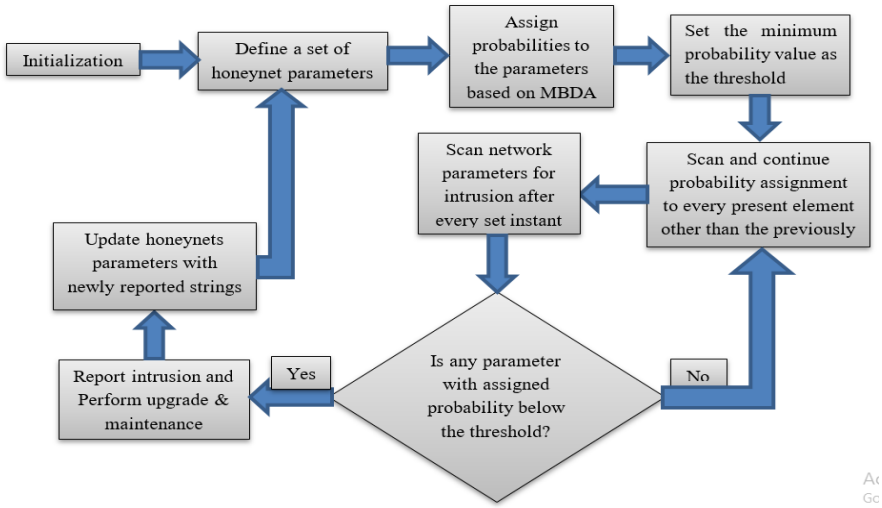


**Figure 5: Intrusion detection scheme by probability assignment of MBDA**

### 2.5. Application of MBDA in AMI for Intrusion Detection

The majority of attacks on AMI in relation to SEM are trying to steal energy through fake signatures or data manipulation. The following are some ways that the proposed MBDA aids in providing real-time SEM intrusion monitoring:

**Step 1** (Initialization): Set potential number of honeynets, $H = \{a(i)\}$ to $n$ and set the number of time steps, counter t = 0.

**Step 2** For each of the monitored SEM, assign probabilities $P_1, P_2 \ldots P_n$ for all possible combinations and set a threshold, $P_0$.

**Step 3** Assign probabilities to all found C&C within a given timestep.

**Step 4** At every set time steps, $t$, and for each of the SEM, Check if $P_i < P_0$ based on defined probability assignment. Return "Intrusion Detected" if True and "No Intrusion Detected" if False.

**Step 5** Report all Smart meters at every time step using the state "1" for intrusion and "0" for no intrusion, report the result to Scenario-based Honeynet Model for further analysis and inferences.

### 2.6. Modelling the Measured Variables

The architecture's monitored parameters are the scheme's observer meter status, δ, timestamps error, β, real-time pricing error, γ, and intrusion detection status, α. Each compromised state in this model is assigned to 1 and the uncompromised state is set to 0. The state of the monitored parameters is first evaluated at a timestep, τ, T as described in Equation (1), where $T_\tau$ is the timestamp at the current evaluation timestep, $T_{\tau-1}$ the timestamp immediately preceding timestamp of evaluation and $s_d$, the variance of the two timestamps. At every timestep $T_d$ must be constant.

As a result, errors are indicated when these variables change, and Equation (2) is used to determine the timestamp inaccuracy β

$$T_\tau - T_{\tau-1} = T_d \quad (1)$$

$$\beta = \begin{cases} 0, & T = T_d \\ 1, & T \neq T_d \end{cases} \quad (2)$$

$P_{1,1}$ ……. $Pn_{,\tau}$ is the real-time price that is given to the neighbourhood at timesteps, 1, 2, 3 to $\tau$ for customers 1, 2, 3 to $n$. Real-time pricing for each of the SEM is verified using Equations (3) through (5), as was previously discussed. Equation (3), is created to ensure constant monitoring of the pricing structure among customers in a zone at any given timestep under the premise that all customers in the Zones are subject to equal per-kWh charging. Equation (4) compares a customer's pricing regime with the utility's rates offered at any τ where $P_{U,\tau}$ indicates the utility's established billing schedule at timestep τ. Equation (5), is developed to define the state for both compromised and uncompromised.

$$\sum_\tau P_{1,\tau} = \sum_\tau P_{2,\tau} = \sum_\tau P_{3,\tau} = \cdots \sum_\tau P_{n,\tau} \quad 3$$

$$\sum_\tau P_{\prec,\tau} = \sum_\tau P_{u,\tau} \quad 4$$

$$\gamma = \begin{cases} 0, & P_{u,\tau} = P_{n,\tau} \\ 1, & P_{u,\tau} \neq P_{i,\tau} \end{cases} \quad 5$$

In order to identify potential compromise in each zone, energy recorded by the observer meter $E_{ob}$, and the energy recorded by all SEM $E_{SEM}$, in the given zone are both monitored at every given timestep. Modelled states of the observer meter, δ, either compromised or uncompromised, are based on values k from Equation (6), where k is the maximum amount of stray or unexplained losses in a zone allowable.

$$\delta = \begin{cases} 0, & E_{ob} - \sum E_{SEM} \leq k \\ 1, & E_{ob} - \sum E_{SEM} > k \end{cases} \quad 6$$

### 2.7. Establishing Security Risks

A low security risk is defined as one monitored parameter becoming compromised, a medium risk as two monitored parameters becoming compromised and a high security risk as all three monitored parameters becoming hacked at once for α, β, and γ while a typical or normal security risk is characterized as one where none of the parameter is allegedly compromised.

**Table 1: Truth table for set rules**

| Scenario | Monitored Parameters | | | Security risk level |
|---|---|---|---|---|
| | A | $\beta$ | $\gamma$ | |
| **1** | 0 | 0 | 0 | Normal |
| **2** | 0 | 0 | 1 | Low |
| **3** | 0 | 1 | 0 | Low |
| **4** | 0 | 1 | 1 | Medium |
| **5** | 1 | 0 | 0 | Low |
| **6** | 1 | 0 | 1 | Medium |
| **7** | 1 | 1 | 0 | Medium |
| **8** | 1 | 1 | 1 | High |

Because any imbalance in the measurements of all the monitored SEM within the zone signals a serious concern, the observer meter gets priority over other monitored parameters. Table 1 is updated using equation (6) to Table 2 with δ and the state of the other parameters remaining unchanged when at state "0" other rules are as captured in Table 2.

**Table 2: Scenario based state parameters for security risk level**

| Scenario | Monitored Parameters | | | | Security Risk Level |
|---|---|---|---|---|---|
| | $\alpha$ | $\beta$ | $\gamma$ | $\sigma$ | |
| **1** | 0 | 0 | 0 | 0 | Normal |
| **2** | 0 | 0 | 0 | 1 | Low |
| **3** | 0 | 0 | 1 | 0 | Low |
| **4** | 0 | 0 | 1 | 1 | High |

| | | | | | |
|---|---|---|---|---|---|
| **5** | 0 | 1 | 0 | 0 | Low |
| **6** | 0 | 1 | 0 | 1 | High |
| **7** | 0 | 1 | 1 | 0 | Medium |
| **8** | 0 | 1 | 1 | 1 | High |
| **9** | 1 | 0 | 0 | 0 | Low |
| **10** | 1 | 0 | 0 | 1 | High |
| **11** | 1 | 0 | 1 | 0 | Medium |
| **12** | 1 | 0 | 1 | 1 | High |
| **13** | 1 | 1 | 0 | 0 | Medium |
| **14** | 1 | 1 | 0 | 1 | High |
| **15** | 1 | 1 | 1 | 0 | High |
| **16** | 1 | 1 | 1 | 1 | Very High |

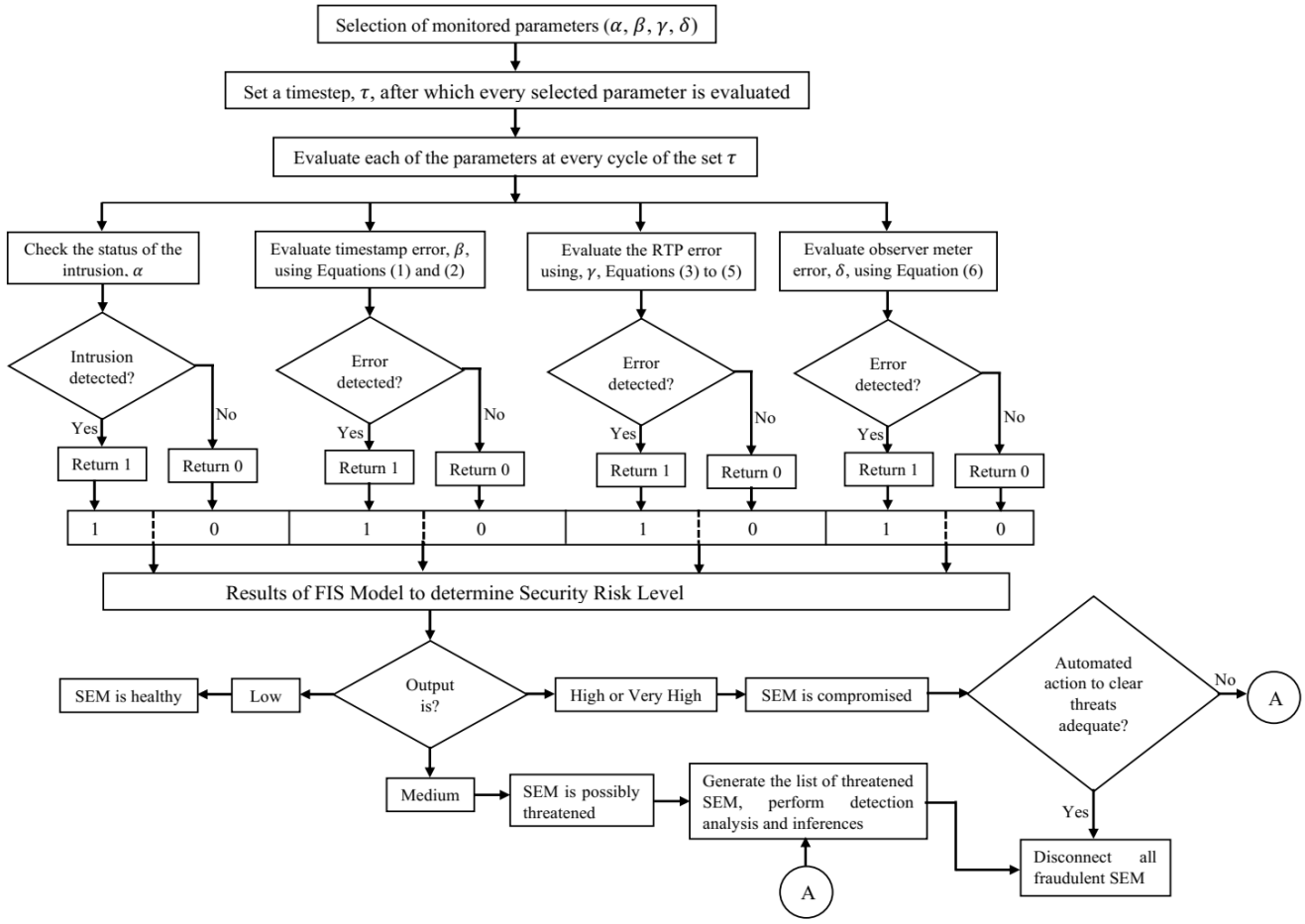


**Figure 6: Implementation of electricity theft prevention model.**

### 2.8. Fuzzy Inference System Design for the Preventative Stage

Using the parameters provided in Table 2 as the basis, a rule-based technique utilizing a fuzzy inference system (FIS) is constructed with the aid of MATLAB to execute the intended monitoring and prevention of electricity theft. Table 2 is used to describe the membership function of the input and output parameters as well as the rules. The input and output structure created using the well-known Mamdani model is shown in Figure 7. The membership functions are triangular and trapezoidal, respectively, for the inputs "Low" and "High," The fuzzy set created for the input and output is displayed in Table 3. Input and output membership functions of the model are depicted in Figures 8 and 9, respectively.

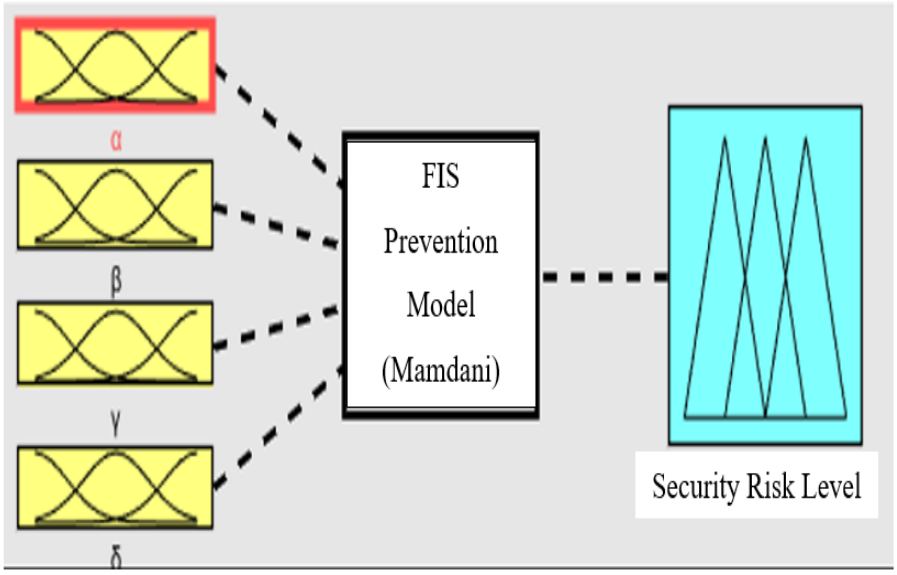


**Figure 7: input-output layout of the developed model**

**Table 3: Defined fuzzy sets for the input and output membership functions**

| | Defined Signal Level | Membership Function | Fuzzy Sets |
|---|---|---|---|
| Input | Low | Triangular | [0 0.3 0.5] |
| | High | Trapezoidal | [0.3 0.5 0.7 1] |
| Output | Normal | Trapezoidal | [0 0.05 0.1 0.2] |
| | Low | Trapezoidal | [0.1 0.2 0.3 0.4] |
| | Medium | Trapezoidal | [0.3 0.4 0.5 0.6] |
| | High | Trapezoidal | [0.5 0.6 0.7 0.8] |
| | Very High | Trapezoidal | [0.7 0.8 0.9 1] |

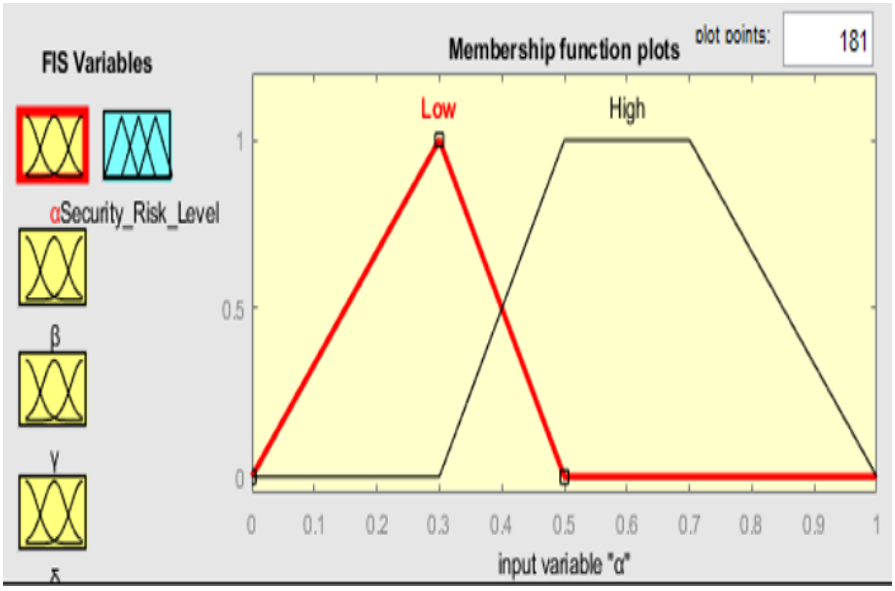


**Figure 8: Input membership function of the developed model for the prevention phase**

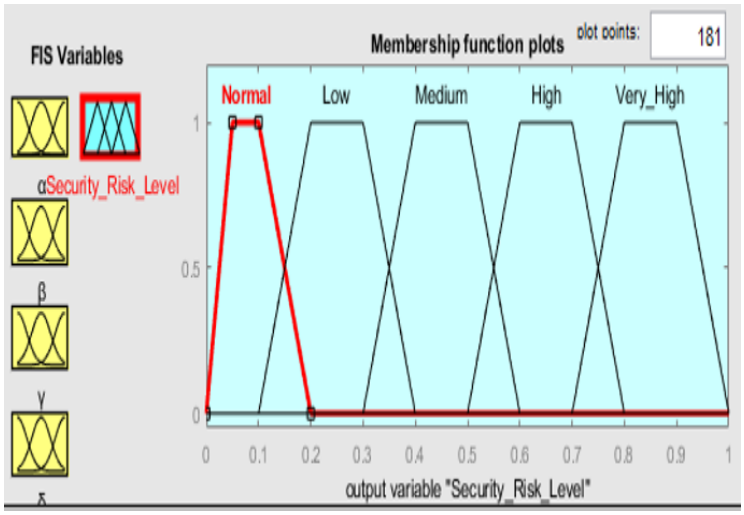


**Figure 9: Output membership functions of the developed model for the prevention phase.**

### 3. Application and Implementation of MBDA

The honeynet set is constructed using a bank of random code generators, and self-attacks are also launched using them. The initial honeynet element count, with a maximum of 10 such that each additional entry causes the oldest record in the honeynet set to be deleted. Then, using Python script, MBDA probability assignment was used to track and report all the self-attacks.

Tables 6 and 7 display the outcomes of two simulations, each with 40 timesteps, and provide information about the timesteps, honeynet element $P_0$, threshold probability, and $Pr(A)$, assigned probability for the intrusive data. For the sake of this demonstration, each timestep is set at 5 s, Table 6 shows the outcome of a single attack. The results of utilizing the script to generate multiple attacks at each represented timestep, applying MBDA to set threshold at each, and locating such intrusion by given probabilities Pr(A) are shown in Table 7.

**Table 6: Implementation of MBDA using a self-Generated script for single attack**

| $\tau$ | $n$ | $P_0$ | Pr$(A)$ | Intrusion detected | | $\tau$ | $\tau$ | $P(o)$ | Pr$(A)$ | Intrusion detected? |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 3 | 0.3333 | 0.000 | FALSE | | 20 | 10 | 0.1000 | 0.0000 | FALSE |
| 1 | 3 | 0.3333 | 0.2500 | TRUE | | 21 | 10 | 0.1000 | 0.0000 | FALSE |
| 2 | 4 | 0.25 | 0.2000 | TRUE | | 22 | 10 | 0.1000 | 0.0000 | FALSE |
| 3 | 5 | 0.2000 | 0.000 | FALSE | | 23 | 10 | 0.1000 | 0.0909 | TRUE |
| 4 | 5 | 0.2000 | 0.1667 | TRUE | | 24 | 10 | 0.1000 | 0.0000 | FALSE |
| 5 | 6 | 0.1667 | 0.1429 | TRUE | | 25 | 10 | 0.1000 | 0.0909 | TRUE |
| 6 | 7 | 0.1429 | 0.0000 | FALSE | | 26 | 10 | 0.1000 | 0.0000 | FALSE |
| 7 | 7 | 0.1429 | 0.0000 | FALSE | | 27 | 10 | 0.1000 | 0.0000 | FALSE |
| 8 | 7 | 0.1429 | 0.0000 | FALSE | | 28 | 10 | 0.1000 | 0.0000 | FALSE |
| 9 | 7 | 0.1429 | 0.0000 | FALSE | | 29 | 10 | 0.1000 | 0.0000 | FALSE |
| 10 | 7 | 0.1429 | 0.1250 | TRUE | | 30 | 10 | 0.1000 | 0.0909 | TRUE |
| 11 | 8 | 0.1250 | 0.0000 | FALSE | | 31 | 10 | 0.1000 | 0.0000 | FALSE |
| 12 | 8 | 0.1250 | 0.1111 | TRUE | | 32 | 10 | 0.1000 | 0.0000 | FALSE |
| 13 | 9 | 0.1111 | 0.0000 | FALSE | | 33 | 10 | 0.1000 | 0.0000 | FALSE |
| 14 | 9 | 0.1111 | 0.0000 | FALSE | | 34 | 10 | 0.1000 | 0.0000 | FALSE |

| 15 | 9 | 0.1111 | 0.0000 | FALSE |
|---|---|---|---|---|
| 16 | 9 | 0.1111 | 0.0000 | FALSE |
| 17 | 9 | 0.1111 | 0.1000 | TRUE |
| 18 | 10 | N/A | 0.0000 | FALSE |
| 19 | 10 | 0.1000 | 0.1000 | TRUE |

| 35 | 10 | 0.1000 | 0.0000 | FALSE |
|---|---|---|---|---|
| 36 | 10 | 0.1000 | 0.0000 | FALSE |
| 37 | 10 | 0.1000 | 0.0000 | FALSE |
| 38 | 10 | 0.1000 | 0.0000 | FALSE |
| 39 | 10 | 0.1000 | 0.0000 | FALSE |

**Table 7: Implementation of MBDA using a Self-Generated script for Multiple attacks**

| $\tau$ | $n$ | $P_0$ | $\Pr(A)$ | Intrusion detected? | | $\tau$ | $n$ | $P_0$ | $\Pr(A)$ | Intrusion detected? |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 3 | 0.3333 | 0.0000 | FALSE | | 20 | 10 | 0.1000 | 0.0000 | FALSE |
| 1 | 3 | 0.3333 | 0.2500 | TRUE | | 21 | 10 | 0.1000 | 0.0000 | FALSE |
| 2 | 4 | 0.2500 | 0.0000 | FALSE | | 22 | 10 | 0.1000 | 0.0000 | FALSE |
| 3 | 4 | 0.2500 | 0.0000 | FALSE | | 23 | 10 | 0.1000 | 0.0000 | FALSE |
| 4 | 4 | 0.2500 | 0.0000 | FALSE | | 24 | 10 | 0.1000 | 0.0000 | FALSE |
| 5 | 4 | 0.2500 | 0.0000 | FALSE | | 25 | 10 | 0.1000 | 0.0000 | FALSE |
| 6 | 4 | 0.2500 | 0.2000, 0.1667 | TRUE | | 26 | 10 | 0.1000 | 0.0000 | FALSE |
| 7 | 6 | 0.1667 | 0.0000 | FALSE | | 27 | 10 | 0.1000 | 0.0909, 0.0833, 0.0769, 0.0714 | TRUE |
| 8 | 6 | 0.1667 | 0.0000 | FALSE | | 28 | 10 | 0.1000 | 0.0000 | FALSE |
| 9 | 6 | 0.1667 | 0.0000 | FALSE | | 29 | 10 | 0.1000 | 0.0000 | FALSE |
| $\tau$ | $n$ | $P_0$ | $\Pr(A)$ | Intrusion detected? | | $\tau$ | $n$ | $P_0$ | $\Pr(A)$ | Intrusion detected? |
| 10 | 6 | 0.1667 | 0.0000 | FALSE | | 30 | 10 | 0.1000 | 0.0000 | FALSE |
| 11 | 6 | 0.1667 | 0.0000 | FALSE | | 31 | 10 | 0.1000 | 0.0909, 0.0833, 0.0769, 0.0714, 0.0667, 0.0625 | TRUE |
| 12 | 6 | 0.1667 | 0.0000 | FALSE | | 32 | 10 | 0.1000 | 0.0000 | FALSE |
| 13 | 6 | 0.1667 | 0.1429, 0.1250, 0.1111, 0.1000 | TRUE | | 33 | 10 | 0.1000 | 0.0000 | FALSE |
| 14 | 10 | 0.10000 | 0.0000 | FALSE | | 34 | 10 | 0.1000 | 0.0000 | FALSE |
| 15 | 10 | 0.10000 | 0.0000 | FALSE | | 35 | 10 | 0.1000 | 0.0000 | FALSE |
| 16 | 10 | 0.10000 | 0.0000 | FALSE | | 36 | 10 | 0.1000 | 0.0000 | FALSE |
| 17 | 10 | 0.10000 | 0.0000 | FALSE | | 37 | 10 | 0.1000 | 0.0000 | FALSE |
| 18 | 10 | 0.1000 | 0.0909, 0.0833 | TRUE | | 38 | 10 | 0.1000 | 0.0000 | FALSE |
| 19 | 10 | 0.1000 | 0.0000 | FALSE | | 39 | 10 | 0.1000 | 0.0000 | FALSE |

## 4. Results Of Rule-Based Model Implementation For The Prevention Phase

The security risk model's outcome, with 0.5 weights assigned to each of the modelled factors, is shown in Figure 10 and is based on the defined states and the FIS-designed model.

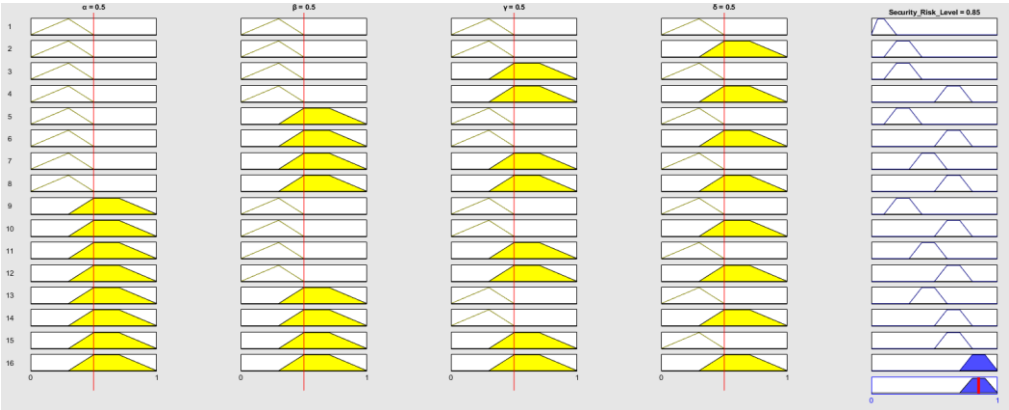

**Figure 10: Rules implementation of FIS-based prevention model**

According to the set rules of which are an exact translation of the scenario-based state parameters used in defining the security risk level as found in Table 2, the selected individual monitored parameter with interdependencies on at least one other parameter with respect to the security level determines the outcome of Figure 10. Threat is high but cover densely in both dimensions where observer meter reading error is large, as seen in Figures 11 to 13, and this pattern is repeated in Figures 14 to 16.

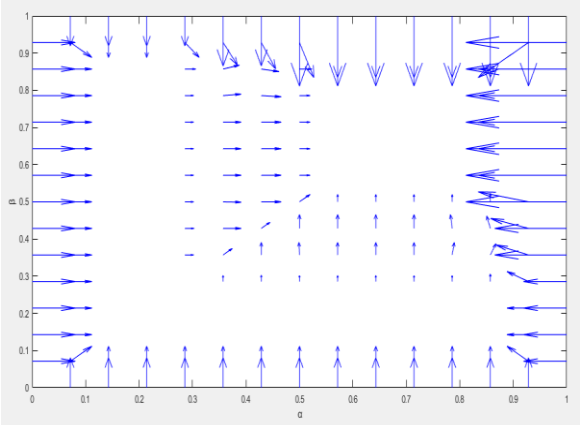

**Figure 11: Model dependency of the intrusion α and timestamp β attacks on the security level**

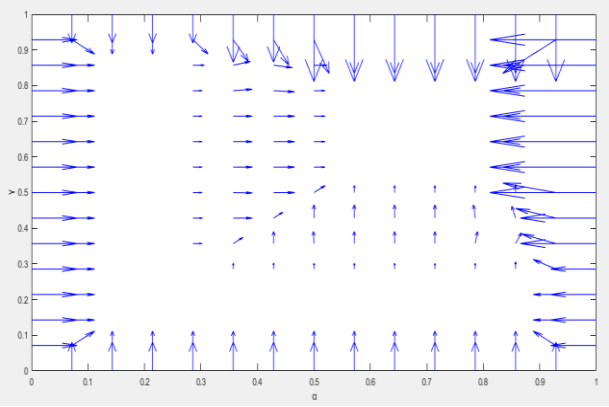

**Figure 12: Prevention model dependency of the real time pricing and intrusion attacks on the security risk level**

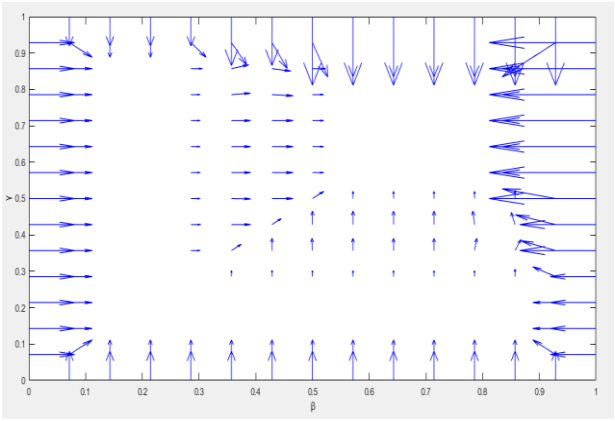


**Figure 13: Prevention model dependency of the real time pricing ($\gamma$) and timestamp ($\beta$) attacks on the security risk level**

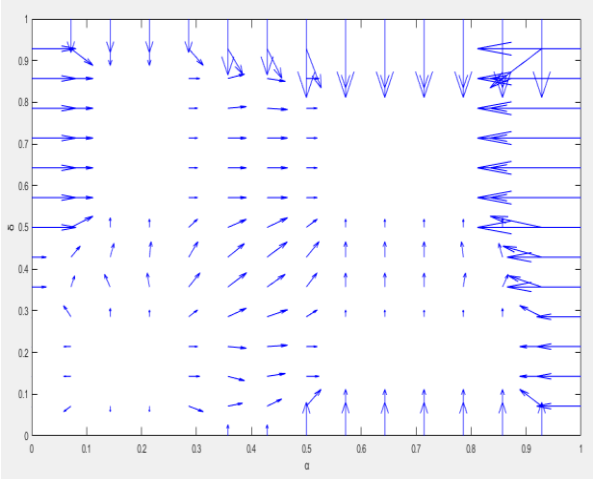


**Figure 14: Prevention model dependency of the observer meter reading status ($\delta$) and intrusion ($\alpha$) attacks on the security risk level**

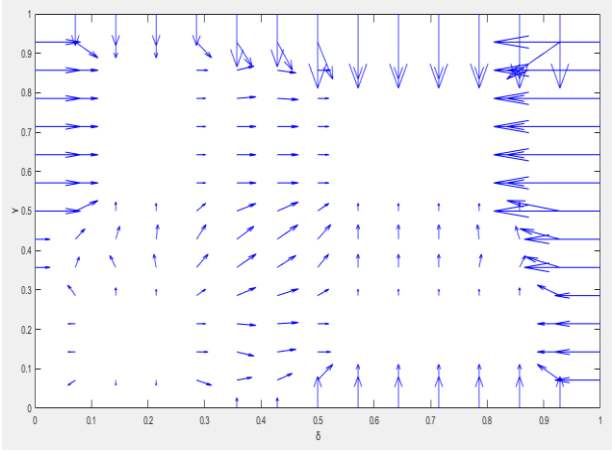


**Figure 15: The prevention model dependency of the observer meter reading status ($\delta$) and real time pricing ($\gamma$) attacks on the security risk levels.**

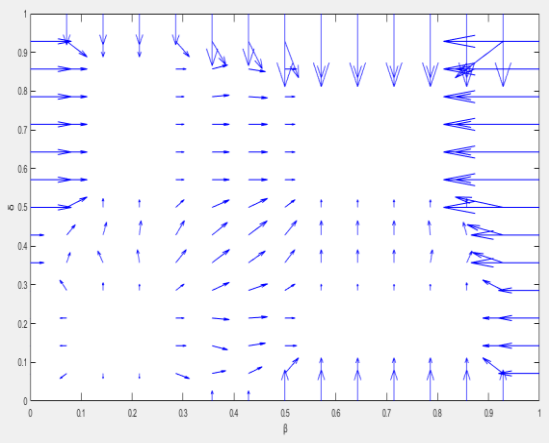


**Figure 16: The Prevention model dependency of the observer meter reading status ($\delta$) and timestamp ($\beta$) attacks on the security risk level**

Based on the outcomes of the FIS model as configured in Figure 6, Table 7 is put into practice. Despite this, attackers are continually looking for ways to break security, necessitating the necessity for provisions for detection in the event of a successful breach. The energy consumption data in kWh, which is the most crucial data in this situation, is thoroughly modelled while presuming that other characteristics have been taken into account in the preventative phase.

## 5. Recommendation and Conclusion

These are the contributions of this study:

i. To track the AMI communication gateways, a unique intrusion detection approach called MBDA is being developed. Through real-time reporting of intrusions, this contributes to adding another layer of protection.

ii. By suggesting a more straightforward AMI monitoring and protection method, the current phony monitoring scheme that invariably results in convoluted and uncoordinated attempts is eliminated. The identification of electricity theft is made simpler if the given clients are divided into zones, as is done in this research. This aids in getting rid of the existing false monitoring technique, which always leads to complicated and disorganized utility activities.

iii. The over-reliance on the use of energy consumption data is reduced by the presentation of the real-time monitoring of consumers for prompt prevention of electricity thefts by the FIS model. Since analysis and monitoring are independent of other consumers in the zone, the availability of customer-dependent models facilitates the monitoring of other network characteristics as appropriate for all consumer types. Additionally, severe errors caused by the practice of creating a common threshold are also eliminated.

Worldwide, electricity theft causes enormous costs and has sparked extensive research into finding remedies, particularly in relation to traditional metering. The greater use of SEM within the SUN via AMI has enhanced security, but it has also raised concerns about electricity theft, necessitating coordinated efforts to find a clever countermeasure to this threat. Unfortunately, the SUN's weakness poses a serious threat to its implementation because it may be easily used to commit crimes like stealing electricity. Despite the difficulties involved and without a doubt unsuitable for a SUN, on-site confirmation is used to confirm dishonest consumers with dubious profiles. Therefore, this work offers a proactive method of reducing electricity thefts in a SUN by rule based preventive measures.

A fresh intrusion detection algorithm is implemented in the preventive phase to assist in adding an extra layer of security to the networks' base IPS. The n-monkey theory, which was developed into scenarios and mapped as the statistical probability assignment method known as MBDA, is used in this algorithm. It was used to detect intrusions at the control and command gateways by applying a predetermined threshold and dynamically assigning

probability to a group of honeynet elements. Another layer of security is also provided by the work, which models the observer meter status, time stamps, and real-time pricing errors in a segmented zone of a neighbourhood network as indicators of electricity thefts. FIS, a rule-based technique, was used to establish security risks and monitor these parameters in order to find and stop any potential theft.

Therefore, this system offers new, proactive, and more thorough ways to detect electricity thefts in a SUN.

## 6. REFERENCES


1. Adhikari, R., and Agrawal, R. K. (2013). An Introductory Study on Time Series Modeling and Forecasting. A*rXiv Preprint*, arXiv:1302.6613.
2. Ahmad, A., Hassan, M., Abdullah, M., Rahman, H., Hussin, F., Abdullah, H., et al. (2014). A Review on Applications of ANN and SVM for Building Electrical Energy Consumption Forecasting. *Renewable and Sustainable Energy Reviews,* 33, 102-109.
3. Ahmad, T., and Ul Hasan, Q. (2016). Detection of Frauds and Other Non-technical Losses in Power Utilities using Smart Meters: A Review. *International Journal of Emerging Electric Power Systems,* 17(3), 217-234.
4. Al-Dhubhani, N. R., and Saeed, F. (2015). A Prototype for Network Intrusion Detection System using Danger Theory. *Jurnal Teknologi,* 73, 8.
5. Alahakoon, D., and Yu, X. (2016). Smart Electricity Meter Data Intelligence for Future Energy Systems: A survey. *IEEE Transactions on Industrial Informatics,* 12(1), 425-436.
6. Alguliyev, R., Imamverdiyev, Y., and Sukhostat, L. (2018). Cyber-Physical Systems and their Security Issues. *Computers in Industry,* 100, 212-223.
7. Amin, M. (2000). Toward Self-Healing Infrastructure Systems. *Computer,* 33(8), 44-53.
8. Amin, M. Challenges in Reliability, Security, Efficiency, and Resilience of Energy Infrastructure: Toward Smart Self-healing Electric Power Grid. *Proceedings of the Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century.* Pittsburgh, PA, USA: IEEE. 2008, 1-5.
9. Amin, S. M. Smart Grid Gecurity, Privacy, and Resilient Architectures: Opportunities and Challenges. *Proceedings of the 2012 IEEE Power and Energy Society General Meeting.* San Diego, CA, USA: IEEE. 2012, 1-2.
10. Amin, S. M., and Wollenberg, B. F. (2005). Toward a Smart Grid: Power Delivery for the 21st Century. *IEEE Power and Energy Magazine,* 3(5), 34-41.
11. Anderson, M. (2010). WiMax for Smart Grids. *IEEE Spectrum, 47*(7), 14-14.
12. Angelos, E. W. S., Saavedra, O. R., Cortés, O. A. C., and de Souza, A. N. (2011). Detection and Identification of Abnormalities in Customer Consumptions in Power Distribution Systems. *IEEE Transactions on Power Delivery,* 26(4), 2436-2442.
13. Arefifar, S. A., Mohamed, Y. A.-R. I., and EL-Fouly, T. H. (2013). Comprehensive Operational Planning Framework for Self-healing Control Actions in Smart Distribution Grids. *IEEE Transactions on Power Systems,* 28(4), 4192-4200.
14. Atif, Y., Jiang, Y., Jianguo, D., Jeusfeld, M., Lindström, B., Andler, S., et al. Cyber-Threat Analysis for Cyber-Physical Systems: University of Skövde. 2018.
15. Baheti, R., and Gill, H. (2011). Cyber-physical Systems. *The Impact of Control Technology,* 12(1), 161-166.