IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 17 January 2024, accepted 9 February 2024, date of publication 26 February 2024, date of current version 7 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3370239

RESEARCH ARTICLE

A Novel Approach Based on Machine Learning, Blockchain, and Decision Process for Securing Smart Grid

NABIL TAZI CHIBI, OMAR AIT OUALHAJ, WASSIM FASSI FIHRI, AND HASSAN EL GHAZI
STRS Laboratory, National Institute of Posts and Telecommunications, Rabat 10140, Morocco
Corresponding author: Nabil Tazi Chibi (tazichibi.nabil@inpt.ac.ma)

ABSTRACT Smart Grids (SGs) rely on advanced technologies, generating significant data traffic across the network, which plays a crucial role in various tasks such as electricity consumption billing, actuator activation, resource optimization, and network monitoring. This paper presents a new approach that integrates Machine Learning (ML), Blockchain Technology (BT), and Markov Decision Process (MDP) to improve the security of SG networks while ensuring accurate storage of events reported by various network devices through BT. The enhanced version of the Proof of Work (PoW) consensus mechanism ensures data integrity by preventing tampering and establishing the reliability of known and unknown attack detection. The proposed versions of PoW, namely GPoW 1.0 and GPoW 2.0, aim to make the consensus process more environmentally friendly.

INDEX TERMS Smart grid, cybersecurity, NIST, vulnerabilities, Markov decision process, blockcahin, machine learning.

I. INTRODUCTION

Smart Grid (SG), also called Smart Electrical Network, was first implemented in Italy in 2005 with the Telegestore project [1]. The objective is, firstly, to promote the consumption of green energy in order to avoid the use of fossil fuels, which currently generate most of the world's primary energy [2]. Secondly, to enable consumers to become producers of this type of energy. The surplus of this energy could be fed into the electricity grid. This concept is a revolution in the field of electricity, where three levels interact: The electrical network, the telecommunications network and information technology. The control and monitoring of this network requires the introduction of technologies used in Industry 4.0, such as IIOT (Industrial Internet of Things), SCADA (System Control and Data Acquisition), SIEM (System Information Event Management) and data analytics [3].

The big data (BD) generated by smart meters (installed in homes to track and bill the amount of electricity consumed and fed into the grid), IIOT and various SG network devices requires a very advanced security policy to guarantee the availability, confidentiality and integrity of the information. According to [4] and [5], the security of an SG could be attacked mainly by Wormholes, Flooding, Puppet attacks, Man in Middle attacks, Password theft, Spoofing, Replay, Data injection and Data modification.

The objective of our paper is to employ Blockchain Technology (BT) in conjunction with the Machine Learning (ML) paradigm and the Markov Decision Process (MDP). In the initial phase, ML will be utilized to categorize validators participating in the Proof of Work (PoW) consensus into two groups: Potential Winners and Potential Losers. Subsequently, in the second phase, we will employ MDP to formulate the optimal policy for Potential Winners. This policy aims to streamline the competition by retaining only those validators with the highest likelihood of success in validating and storing events in the BT Ledger. The ultimate goal is to make our consensus model more environmentally sustainable.

This paper is structured as follows. In Section II, we introduce the smart grid domains and their vulnerabilities. In Section III, we discuss some related work.

The associate editor coordinating the review of this manuscript and approving it for publication was Xianzhi Wang.

Section IV presents our methodology. In Section V we highlight the results obtained and finally in Section VI we conclude and present some perspectives.

II. SMART GRID AND CYBER-SECURITY

A. SMART GRID OVERVIEW

The National Institute of Standard and Technology (NIST) [14] has proposed a conceptual model (see Fig. 1) which makes it possible to clearly identify the different components, actors and actions that are involved in an SG network. The NIST model of the SG is organized into seven domains [19]:

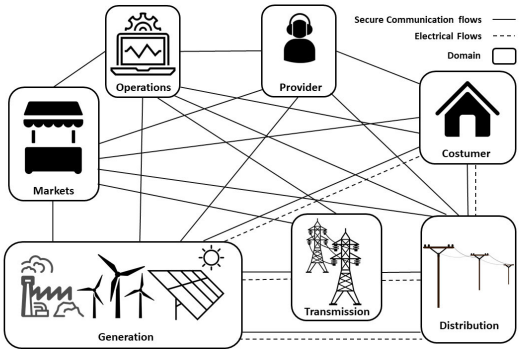

FIGURE 1. Smart grid's framework based on NIST.

- Generation: The production of the electricity using traditional and ecological technologies.
- Transmission: The transmission of electricity over long distances. With the ability to generate and store the electricity.
- Distribution: distribution of electricity to and from the end users.
- Markets: Electricity market participants for better sales.
- Consumer: Traditionally, the end user's role was to consume electricity. In this new configuration, they could generate, store, deliver and manage energy.
- Operations: managing the flow of electricity.
- Provider: providing services to utilities and customers.

B. SMART GRID VULNERABILITIES AND COUNTERMEASURES

The cybersecurity objectives for the SG, as defined by NIST [14] are:

- confidentiality: protecting the SG from attacks that tries to access to private data
- Availability: keeping the information accessible
- Integrity: ensuring that the data is not altered

The main sources of vulnerability in an SG [16] are software with security flaws, incorrect configurations, unprotected communication lines, lack of maintenance, an unprotected network, etc.

Attacks on an SG could be at the level of components, communications and protocols [15], [20] or topologies. These attacks could take several forms [24], [25], such as: Malware and virus spreading, database links, communication hijacking, replay attack with false data injection, Modbus protocol privacy, interception of network traffic, unplanned shutdown [17].

There are best practices in the literature to counter-attacks such as [18] and [23], disabling unused services and software, controlling access to resources, changing default passwords and accounts, using complex passwords, using logging to monitor activity, restricting communication on a segmented network, protecting against malware, sending regular signals (Heartbeat Signals) by the components to indicate that their state is normal, installing equipment that conforms to standards, using anonymous key agreement and mutual authentication protocol [39], dynamic ephemeral and session key generation protocol [40], lightweight authentication mechanism [41], cryptographic for safeguarding information and communication [42], [43] . . . etc.

In this work, we want to guarantee the reliability of the events generated by the network equipment by storing these data using the BT. We will therefore start by studying works in which the BT has been used in the SG field.

III. RELATED WORK

Through the study of work carried out on BT and its use in smart grid networks, we find that it mainly affects the operational aspect [6]. To summarize, this technology could be used:

- To secure the AMI (Advanced Metering Infrastructure) transactions. The Blockchain has been tested in storing data related to the energy consumed for billing reasons and applying the rules defined by the operator through smart contracts.
- On Trading and Market, to secure energy sales transactions between individuals without third-party intermediaries.
- For monitoring and control to enforce the reliability of data that maintains the proper functioning of the infrastructure components.
- To ensure the non-alteration of data used in an electrical protection platform, called an Adaptive Protection Platform (APP) [7].
- For storing data from smart sensors based on Ethereum technology and applying certain rules using smart contracts [8].
- To regulate the communication between the utility and the smart meters based on the smart contract [9].
- To Secure the storage of events coming from IOTs on a Smart Grid Network using PoW Consensus [10].
- For the management, control and operation of an SG Network [11].

Upon scrutinizing the existing literature and conducting a comparative analysis of the technologies enumerated in Table 1 for securing the smart grid, it is evident that none of these researches have integrated all three technologies: Blockchain Technology (BT), Machine Learning (ML), and Markov Decision Process (MDP) to enhance the energy efficiency of the Proof of Work (PoW) consensus while

concurrently establishing an effective security framework for the smart grid. This unique combination is a novel aspect that our paper endeavors to explore and contribute to the existing body of knowledge.

TABLE 1. Comparison of the technologies used (BT, ML and MDP) to secure the SG in related work.

Related Work	BT	ML	MDP	Comment
[33]	X			BT proposed as a solution to secure SG
[34]	X			BT and smart contracts to improve the reliability of transactions
[33]	X			Secure data awareness model using blockchain
[36]	X			Proposal of an abstract system for the prevention of data injection
[37]	X	X		In this survey, AI/ML and BT were identified as a solution for cybersecurity chalenges
[27]	X	X		BT ledger with an AI-enabled secure framework for SG
[28]	X	X		Analysing solutions using different methods based on IA/ML and BT
[29]	X	X		Proposal of a model to improve the security of the SG based on the BT, and industrial fault detection using wireless sensors Network and deep learning techniques
[44]	X			Securing industrial IoTs data in the Electric SG using a blockchain-based system

Our objective and contribution revolve around enhancing the energy efficiency of the Proof of Work (PoW) consensus, a concept often acknowledged as energy-intensive in existing literature [31]. Simultaneously, we aim to establish a sustainable security model for the smart grid. To achieve this, we propose the utilization of Machine Learning (ML) and Markov Decision Process (MDP) to create two environmentally friendly versions of PoW, namely GPoW 1.0 and GPoW 2.0. These versions will be instrumental in storing events generated by Smart Grid (SG)-enabled devices. The integration of Blockchain Technology (BT) ensures the protection of all stored data, maintaining transaction integrity and eligibility.

IV. METHODOLOGY

Our approach will be based on blockchain technology (BT) to store events from SG devices in a decentralized way employing machine learning [26] and the Markov decision process in order to reduce energy consumption and for better load balancing between nodes, ensuring validation and storage of these events.

A. MACHINE LEARNING

The Machine Learning [21] Fig.2, in our approach, will help us to develop a Prediction Model (PM) from experimental Data (Dataset) based on a Supervised Learning techniques using a Classification Model that allows to identify which category an object belongs to.

B. BLOCKCHAIN TECHNOLOGY

Blockchain technology [22] is based on a distributed data storage and processing, which avoids the monopoly of power by a single authority. This storage and processing

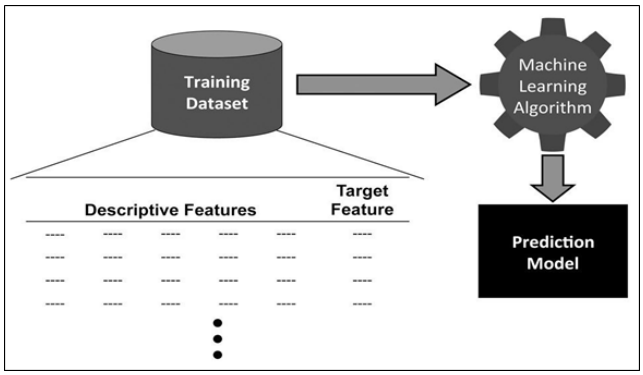

FIGURE 2. Machine learning workflow.

will be carried out by several nodes/computers on the network. The data will be formatted and stored as a chain of blocks in a decentralized way, called DLT (Distributed Ledger Technology). The Blockchain has mechanisms that will ensure that this data will be unaltered within a redundant system that is resilient to failures and cyber-attacks. Blockchain technology could be public or private and it is based on different types of consensuses for the validation and insertion of new blocks in the Blockchain, such as [6] and [12]:

- Proof of Work (PoW): Here the nodes are called miners and must solve a calculation of a very complicated problem, the node which finds the solution first broadcasts it to the other nodes for verification and insertion in the distributed ledger (DL). The disadvantage of this consensus is the very high energy consumption. This consensus is used by the Bitcoin.
- Proof of Stake (PoS): Here the nodes are called Validators. Block validation is randomly granted to nodes that have the most and oldest shares.
- Delegated Proof of Stake (DPoS): In this consensus, the validators will be a subset of the PoS validators for whom the task of validation will be delegated.
- Leased Proof of Stake (LPoS): Here, nodes lease their assets to other nodes to increase the probability of being a validator. Profits will be shared among the members of each node group.
- Proof of Activity (PoAc): It is a consensus that start by using PoW and once the miners reap enough rewards the system switches to PoS using the rewards as stakes.
- Proof of Burn (PoB): Validators will need to regularly burn some of their own coins to increase their chances of being selected. This action is done by sending some coins to public and verifiable addresses. This consensus is used by the Slimcoin.
- Proof of Authority (PoA): Validators will be pre-selected and authorized to validate blocks based on their identity. Etherum is based on this type of consensus.

Other consensus variants exist like: Proof of Inclusion (PoI), Proof of Elapsed Time (PoET) and Practical Byzantine Fault Tolerance (PBFT).

C. MARKOV DECISION PROCESS APPROACH

The MDP (Markov Decision Process) [13] allows the modelling of a process for decision-making assistance. At a given time, the process is in a state S. Several actions will be possible in this state, the decision maker must choose an action a among them. The process will react by moving randomly (according to a probability $P_a(S, S')$) to another state S' and will offer a reward $r_a(S, S')$ to the decision maker.

The goal will be to find the optimized policy for the decision maker.

D. OUR APPROACH

The advantage of our work is to propose a model based on PoW consensus enhanced by some adaptations to make it very energy efficient. In our model, the authority will be granted to a certain number of validators, which will compete to validate and store in the Blockchain ledger the received event to maximize the profit by deciding at each state the action to be taken (bet or not bet) depending on the conditions and the context. Our model will have the advantage of not consuming too much energy and helping validators to make the right decisions at each time, by using ML and MDP for better resource optimization and fair benefit sharing.

E. OUR ARCHITECTURE

In this work, we will focus on the equipment installed in private homes because, in our opinion, they pose the most security risks due to several reasons, such as willingness to falsify bills, the types of equipment are not being updated or are not compliant with the standard, the local area network (LAN) is not protected, and other such factors. In our Fig.3 architecture, we consider that the customer (e.g., a house) has mainly several IoTs and a smart meter connected to its LAN that uses a home router to communicate with the electricity provider via the Internet.

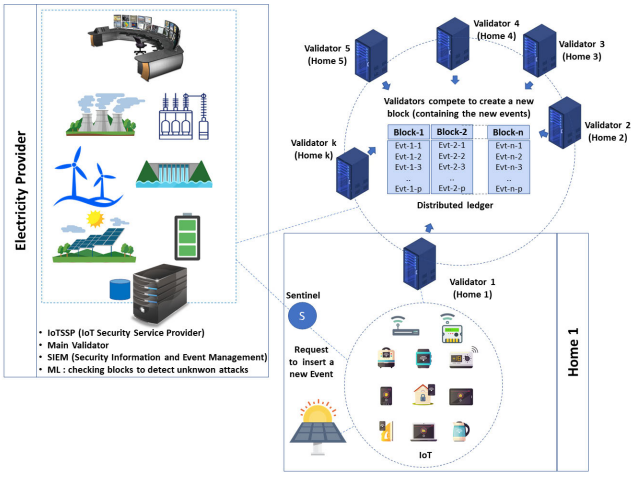

FIGURE 3. Proposed architecture to secure smart grids.

The events generated by the IoTs and Smart Meter will cross the sentinel, which is responsible for centralizing events and transferring them to the IoTSSP (IoT Security Service Provider) which will either authorize the processing of the event or will block it based on a blocklist and the Machine Learning Algorithms as presented in the flow chart Fig.4.

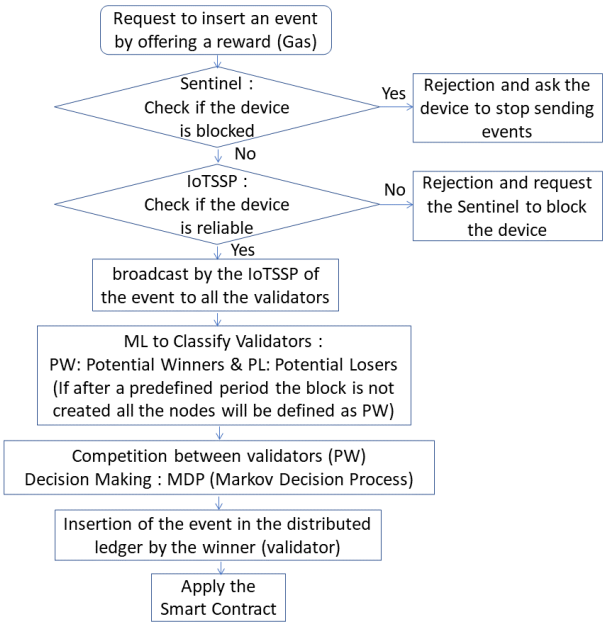

FIGURE 4. Flow chart – inserting an event.

If the event is legitimate, the IoTSSP broadcasts the event to all the validators to launch the competition between several nodes validators (NV) of the network whose objective is to maximize their profit by winning the reward (Gas) offered by the equipment which generated the event. The winner will validate the event and ask the other nodes to store this event in a decentralized way based on BT.

In order to make the competition between the nodes significantly less energy-intensive, we will use an improved version of the PoW consensus that we will call GPoW (Green Proof of Work). This consensus will use ML to classify nodes based on a list of futures and history. A node before deciding to compete and thus consuming energy, It will estimate its chances to win using ML, the node will be classified as potential winner (PW) or potential loser (PL).

We will produce two versions of the GPoW consensus, GPoW 1.0, where the ML layer is added to the classical PoW consensus, and GPoW 2.0, which is an improved version of the GPoW 1.0 because we add the Markov Decision Process.

F. GPoW 1.0: ADDING THE MACHINE LEARNING LAYER

When an event is broadcasted, the nodes receive as information: EventSource, Gas and TTL. Where:

- EventSource: The ID of the device that sent the event
- Gas: The gas offered by the device for the validation of the event
- TTL: The TTL field will have a given value on an IP packet when the device sends it. This value will be decremented each time the packet passes through a router on the Internet network. Once arrived at the destination, it will allow for estimating the time elapsed before the packet's arrival.

The features that will allow us to apply machine learning will be the information received and listed above, plus the following three features:

- TimeFrameImpact: The day will be divided into twelve time slots of two hours. Initially, the value of the TimeFrameImpact variable will be fifty for all nodes and on all slots. After each processing request (Addition of an event in the Blockchain), the value of the TimeFrameImpact variable will be re-evaluated for all nodes on the slot corresponding to the processing time. We will remove points (one for example) for the losing nodes, and we will add points (one for example) for the winning node, with zero as the minimum and a hundred as the maximum value of the TimeFrameImpact.
- CPU: The available CPU of the node
- Memory: The available memory of the node
- Bandwidth: The available bandwidth of the node

Each validator will have his features (Gas, TTL, TimeFrameImpact, CPU, Memory, Bandwidth) to be able to apply the prediction model locally (which will be updated regularly based on previous results) for a self-classification (PW or PL) to decide whether to participate or not. This classification would normally eliminate numerous potential losers, which would have a very significant impact on reducing energy consumption.

G. GPoW 2.0: APPLYING THE MARKOV DECISION PROCESS

In order to make it clear, we will apply our approach on 2 use cases, in the first one we will consider that all the validators are identical and in the second one, we will have 2 kinds of validators.

Model 1: The Blockchain validators are identical

Scenario description:

We assume that we have n validators/players.

- Each player has 2 possible actions:
  - 1: to bet
  - 2: wait (do not bet)
- The player can switch between 2 states:
  - F: Free
  - B: Busy
- We will focus on one validator V. Because the scenario is the same for the other validators.
- We will consider that:
  - b: The bet value
  - r: The reward value
  - p: The probability that a validator V who has bet to be chosen from among all the validators who have bet

Based on the probability tree Fig.5, we can deduce the probability p.

The probability p can be calculated through the formula (1), below:

$$p = \sum_{m=1}^{n} \frac{1}{m} \times \frac{C_{n-1}^{m-1}}{\sum_{k=0}^{n} C_n^k} \tag{1}$$

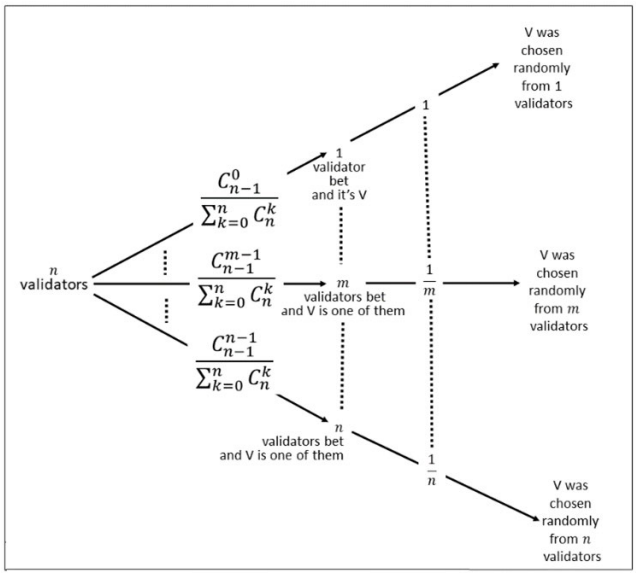

FIGURE 5. Probability tree – the validators are identical.

The competition between validators could be schematized through the Markov Decision Process (Fig. 6).

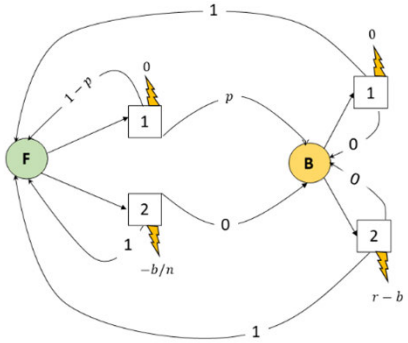

FIGURE 6. Markov decision process – the validators are identical.

Our model is based on the formulas 1, 2, 3, 4 and 5.

$$P(.;.;1) = \begin{bmatrix} 1-p & p \\ 1 & 0 \end{bmatrix} \tag{2}$$

$$P(.;.;2) = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \tag{3}$$

$$U(.;1) = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \tag{4}$$

$$U(.;2) = \begin{bmatrix} \frac{-b}{n} \\ r-b \end{bmatrix} \tag{5}$$

where:

- $P(.;.;1)$ defines the transition matrix to go from a state to another one if the player decides to bet (1). These transitions are well schematized in Fig.6.
- $P(.;.;2)$ defines the transition matrix to go from a state to another one if the player decides not to bet (2).
- $U(.;1)$ defines the reward matrix if the player decides to bet (1) in the different possible states (F and B).

- $U(.;2)$ defines the reward matrix if the player decides not to bet (2) in the different possible states (F and B).

Model 2: two kinds of Blockchain validators

Scenario description:

- We assume that we have n validators/players and that $n = n_s + n_f$
- n_s players from n players could bet b_s and b_f, such as: $b_s > b_f$.
- n_f players from the n players could bet only b_f, such as: $b_s > b_f$.
- The player who has bet in a state will not be able to bet in the next state.
- We will focus on the n_s validators, because for the n_f validators the decision will be simple for them: They have to bet b_f each time.
- Each player can be Free (F) or Busy (B) or Saturated (S)
  - Free: all the resources of the player are available
  - Busy: The player bet a part of his resources b_f, such as $(b_s > b_f)$
  - Saturated: The player bet all his resources b_s, such as $(b_s > b_f)$
- A reward will be randomly: r_s or r_f and we assume that $r_f < r_s$
- The possible states are: (F;r_f); (F;r_s); (B;r_f); (B;r_s); (S;r_f); (S;r_s)
- $p(r_f)$ is the probability that r_f occurs and $p(r_s)$ is the probability that r_s occurs.
- We consider that when the reward is r_f and a player bet, the value of his bet will be b_f. When the reward is r_s and a player bet, the value of his bet will be b_s.
- Actions are: 1: bet; 2: Wait
- For the winner:
  - The payoff will be (r_f-b_f) or (r_s-b_s)
  - And we assume that (r_f-b_f) < (r_s-b_s)
- p_f is the probability for a player who bet b_f to be chosen. And p_s is the probability that one of the n_s players who bet b_s to be chosen.
- Our objective is to find the best policy for the n_s players to maximize their total payoffs.

Whatever the action chosen in the states (B;r_f), (B;r_s), (S;r_f) and (S;r_s) the user will return to the starting box either to (F;r_f) or (F;r_s), depending on the probabilities $p(r_f)$ and $p(r_s)$.

The competition between validators could be schematized through the Markov Decision Process (Fig. 7).

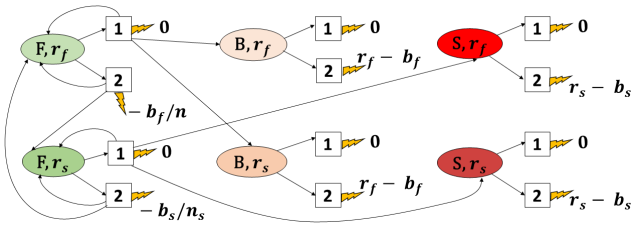

FIGURE 7. Markov decision process – 2 categories of validators.

Our model is based on the (6)–(11), as shown at the bottom of the next page, where:

- $P(.;.;1)$ defines the transition matrix to go from a state [(F;r_f); (F;r_s); (B;r_f); (B;r_s); (S;r_f); (S;r_s)] to another one if the player decides to bet (1).
- $P(.;.;2)$ defines the transition matrix to go from a state to another one if the player decides not to bet (2).
- $U(.;1)$ defines the reward matrix if the player decides to bet (1) in the different possible states.
- $U(.;2)$ defines the reward matrix if the player decides not to bet (2) in the different possible states.

V. RESULTS AND DISCUSSIONS

A. GPoW 1.0: SIMULATION RESULTS:

We apply our approach to 10 nodes, taking into account the time factor. When starting our simulation, we consider that the impact of time slots is identical (=50) for the different nodes. In each loop, we add one point (+1) to the time slot impact if the node won, and we subtract one point (−1) from the time slot impact if the node loses. After a while, we found ourselves with the Table.2 as time slot impacts.

TABLE 2. Slot time impacts on the potential gain or loss of nodes.

	Node1	Node2	Node3	Node4	Node5	Node6	Node7	Node8	Node9	Node10
00h-02h	94	40	31	89	36	76	39	53	46	53
02h-04h	11	33	74	59	25	50	43	6	75	14
04h-06h	30	29	70	5	78	77	17	66	62	54
06h-08h	52	14	26	7	19	47	89	31	87	39
08h-10h	48	93	89	41	25	94	66	86	29	43
10h-12h	66	48	68	24	29	71	20	72	75	31
12h-14h	34	10	30	46	48	91	67	58	52	25
14h-16h	83	58	57	75	68	10	74	80	15	86
16h-18h	87	76	95	63	43	57	27	10	7	94
18h-20h	68	46	87	86	9	9	49	61	9	25
20h-22h	45	31	88	18	76	75	83	16	7	41
22h-24h	92	39	44	30	17	46	93	51	40	60

We consider that we are launching the competition between these 10 nodes in the different time slots for different Gas values (integer numbers ranging from 10 to 100). These nodes will have different performance in terms of memory, processor and bandwidth. The TTL (Time To Live) will be influenced by the path traced by the event packet. This simulation will generate a dataset of more than 10000 lines, with as features: Gas, TTL, TimeFrameImpact, CPU, Memory, Bandwidth. The label of these features will be 1 (if the node win) and 0 (if the node lose)

Based on this dataset and applying ML, we can predict for a given node whether it is a potential winner or a potential loser. We use the KNeighbors classifier and the GaussianNB model, which have accuracies exceeding 0.93. The competition will be between the limited number of potential winners.

B. GPoW 2.0: MODEL 1 - SIMULATION RESULTS

Through the application of the Reinforcement Learning Algorithm, and by varying the values of n (the number of validators), r (the value of the reward) and b (the value of the bet), we always find that the optimal policy is:

- If the node is in state F (Free) it is recommended to bet
- If the node is in state B (Busy) it is recommended not to bet

C. GPoW 2.0: MODEL 2 - SIMULATION RESULTS

We set all the parameters and we vary the value of the higher bet: $b_s \in [2..10]$; $n = 7$; $n_s = 3$; $r_f = 3$; $r_s = 10$; $b_f = 2$; $p(r_f) = 2/3$; $p(r_s) = 1/3$

The results are visible in the graph below (Fig. 8).

We notice that in this case the rate of the occupancy of the different states by the validators with the higher performance remains fixed. This will only impact the payoff of the validator.

In the second simulation, we set all the parameters and we vary the number of validators with the higher performance: $n_s \in [1..10]$; $n = 10$; $r_f = 4$; $r_s = 10$; $b_f = 2$; $b_s = 6$ $p(r_f) = 2/3$; $p(r_s) = 1/3$

The results are visible in the graph below (Fig. 9).

With the increase in the number of the validators with higher performance, we notice that the occupancy rate of stages (S;r_f) and (S;r_s) decreases and that it increases for stages (F;r_f) and (F;r_s). On the other hand the rate of stages (B;r_f) and (B;r_s) remains stable.

In the third simulation, we set all the parameters and we vary the Probability that r_s (a superior reward) occurs: $p(r_s) \in [0, 1 : 0, 1 : 0, 9]$; $n = 10$; $n_s = 4$; $r_f = 4$; $r_s = 10$; $b_f = 2$; $b_s = 6$; $p(r_f) = 1\text{-}p(r_s)$

TABLE 3. Example of 10 nodes at a given time.

Node	TimeFrameImpact	CPU	Memory	Bandwidth	TTL	Gas
Node1	94	1	8	54	82	10
Node2	85	1	8	36	41	10
Node3	92	1	8	40	28	10
Node4	89	1	8	40	87	10
Node5	36	1	8	23	59	10
Node6	76	1	8	53	39	10
Node7	39	1	8	50	6	10
Node8	53	3	32	33	71	10
Node9	82	2	16	68	15	10
Node10	53	3	32	22	11	10

The results are visible in the graph below (Fig. 10).

With the increase of this probability, we notice that the occupancy rate of stages (S;r_s) increases. The aim of these simulations is to see the effect of the conditions (value of the bet, number of nodes, frequency of the different rewards) to increase the chances of the nodes (potential winners selected in the first round using GPoW 1.0) to be in a saturated state, i.e. to win the competition to further reduce power consumption through our GPoW 2.0 consensus proposal.

$$p_f = \sum_{m=1}^{n} \frac{1}{m} \times \frac{C_{n-1}^{m-1}}{\sum_{k=0}^{n} C_n^k} \tag{6}$$

$$p_s = \sum_{m=1}^{n_s} \frac{1}{m} \times \frac{C_{n_s-1}^{m-1}}{\sum_{k=0}^{n_s} C_{n_s}^k} \tag{7}$$

$$P(.;.;1) = \begin{bmatrix} (1-p_f)\times p(r_f) & (1-p_f)\times p(r_s) & p_f \times p(r_f) & p_f \times p(r_s) & 0 & 0 \\ (1-p_s)\times p(r_f) & (1-p_s)\times p(r_s) & 0 & 0 & p_s \times p(r_f) & p_s \times p(r_s) \\ p(r_f) & p(r_s) & 0 & 0 & 0 & 0 \\ p(r_f) & p(r_s) & 0 & 0 & 0 & 0 \\ p(r_f) & p(r_s) & 0 & 0 & 0 & 0 \\ p(r_f) & p(r_s) & 0 & 0 & 0 & 0 \end{bmatrix} \tag{8}$$

$$P(.;.;2) = \begin{bmatrix} p(r_f) & p(r_s) & 0 & 0 & 0 & 0 \\ p(r_f) & p(r_s) & 0 & 0 & 0 & 0 \\ p(r_f) & p(r_s) & 0 & 0 & 0 & 0 \\ p(r_f) & p(r_s) & 0 & 0 & 0 & 0 \\ p(r_f) & p(r_s) & 0 & 0 & 0 & 0 \end{bmatrix} \tag{9}$$

$$U(.;1) = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{10}$$

$$U(.;2) = \begin{bmatrix} \frac{-b_f}{n} \\ \frac{-b_s}{n_s} \\ r_f - b_f \\ r_f - b_f \\ r_s - b_s \\ r_s - b_s \end{bmatrix} \tag{11}$$

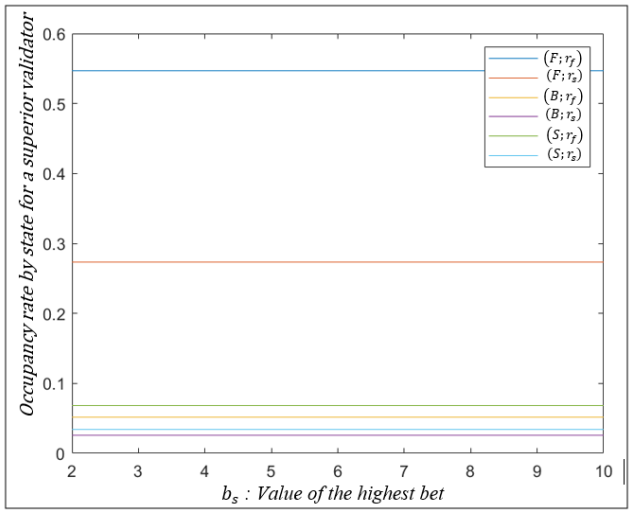

FIGURE 8. Model 2 simulation results.

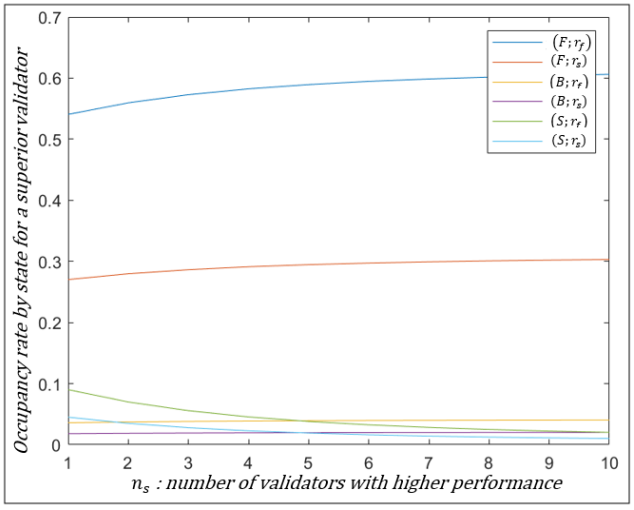

FIGURE 9. Model 2 simulation results.

D. A USE CASE

Let us assume that we have a list of 10 nodes as shown in the table 3.

In the classical PoW, all these nodes must compete to mine the event received.

Using our approach, in the first step (GPoW 1.0 consensus) we apply the ML (Reinforcement Learning) to find the results in the table 4.

We can see that the number of competitors is reduced to 4 nodes.

Now let's use MDP to upgrade to version 2 of our GPoW consensus.

We assume that: $n = 4$; $n_s = 2$; $p(r_s) = 0.3$; $p(r_f) = 0.7$; $r_f = 10$; $r_s = 20$; $b_f = 5$; $b_s = 12$.

Through the policy iteration of MDP algorithm, we find that the optimal policy is that the node must always bet when it's in the Free states ((F;r_f) or (F;r_s)).

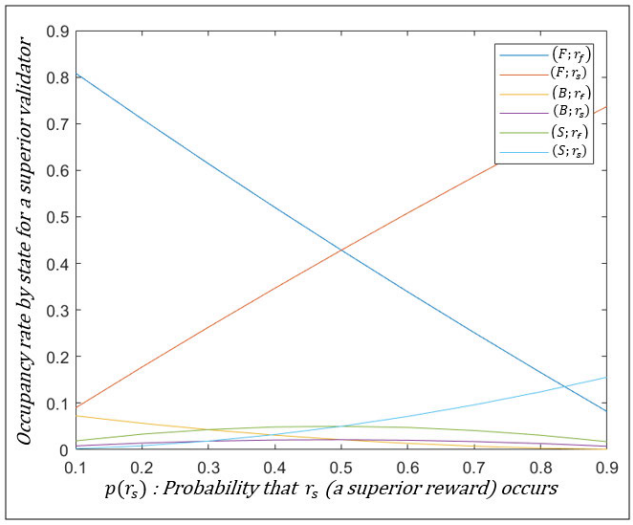

FIGURE 10. Model 2 simulation results.

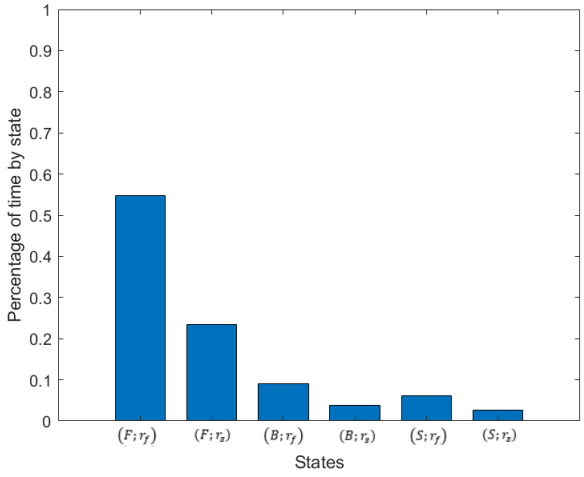

FIGURE 11. Model 2 simulation results.

TABLE 4. Results using GPoW 1.0 consensus.

Node	Result
Node1	Potential loser
Node2	Potential loser
Node3	Potential winner
Node4	Potential loser
Node5	Potential loser
Node6	Potential winner
Node7	Potential loser
Node8	Potential loser
Node9	Potential winner
Node10	Potential winner

Using the stationary distribution of MDP algorithm, we can see from the Fig. 11 that the occupancy rate of the free states (the first and second bars) does not exceed 80%, so the node will not bet in 20% of the cases. Which will again reduce energy consumption.

VI. CONCLUSION

Opening smart grids to the Internet requires significant innovation to counter the rapid evolution of attack techniques.

Our approach reliably stores the events generated by the various devices in the smart grid. We decentralise the information by involving the network nodes in the event validation and storage process using an enhanced version of the Proof of Work (PoW) consensus, which we call GPoW 1.0, a proposal that uses machine learning based on historical transactions to allow nodes to predict their potential to win or lose, reducing the number of nodes competing and thus the total amount of energy consumed. Our second version GPoW 2.0, is an improved version of GPoW 1.0, because it will apply on the nodes resulting from this first phase (GPoW 1.0), the algorithms of the MDP to define the best policy for this reduced number of nodes to keep in competition only the nodes with maximum of chance to win, thus making our consensus greener.

As a perspective, we plan to work on the use of events coming from smart grid network devices and stored in a reliable and eco-friendly way, using GPoW 2.0 to use machine learning to detect known and unknown cyber-attacks.

Combining our approach with prior research work [27], [28], [29] rooted in BT and ML opens up the possibility for exploring alternative research avenues, addressing diverse security aspects of SG, or delving into topics like IoT [30], [31], [32] and the cognitive radio [38].

REFERENCES

[1] A. T. Y. Chong, M. A. Mahmoud, F.-C. Lim, and H. Kasim, "A review of smart grid technology, components, and implementation," in *Proc. 8th Int. Conf. Inf. Technol. Multimedia (ICIMU)*, Selangor, Malaysia, Aug. 2020, pp. 166–169, doi: 10.1109/ICIMU49871.2020.9243430.

[2] F. Ayadi, I. Colak, I. Garip, and H. I. Bulbul, "Impacts of renewable energy resources in smart grid," in *Proc. 8th Int. Conf. Smart Grid*, Paris, France, Jun. 2020, pp. 183–188, doi: 10.1109/icSmartGrid49881.2020.9144695.

[3] S. Tripathi, P. K. Verma, and G. Goswami, "A review on SMART GRID power system network," in *Proc. 9th Int. Conf. Syst. Modeling Advancement Res. Trends (SMART)*, Moradabad, India, Dec. 2020, pp. 55–59, doi: 10.1109/SMART50582.2020.9337067.

[4] A. I. Kawoosa and D. Prashar, "A review of cyber securities in smart grid technology," in *Proc. 2nd Int. Conf. Comput., Autom. Knowl. Manage. (ICCAKM)*, Dubai, United Arab Emirates, Jan. 2021, pp. 151–156, doi: 10.1109/ICCAKM50778.2021.9357698.

[5] R. Marah, I. E. Gabassi, S. Larioui, and H. Yatimi, "Security of smart grid management of smart meter protection," in *Proc. 1st Int. Conf. Innov. Res. Appl. Sci., Eng. Technol. (IRASET)*, Meknes, Morocco, Apr. 2020, pp. 1–5, doi: 10.1109/IRASET48871.2020.9092048.

[6] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Y. M. Ghias, L. H. Koh, and L. Yang, "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 18–43, Jan. 2021, doi: 10.1109/JIOT.2020.2993601.

[7] D. Sikeridis, A. Bidram, M. Devetsikiotis, and M. J. Reno, "A blockchain-based mechanism for secure data exchange in smart grid protection systems," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2020, pp. 1–6, doi: 10.1109/CCNC46108.2020.9045368.

[8] Q. Xu, Z. He, Z. Li, and M. Xiao, "Building an Ethereum-based decentralized smart home system," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Singapore, Dec. 2018, pp. 1004–1009, doi: 10.1109/PADSW.2018.8644880.

[9] R. Akhras, W. El-Hajj, M. Majdalani, H. Hajj, R. Jabr, and K. Shaban, "Securing smart grid communication using Ethereum smart contracts," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Limassol, Cyprus, Jun. 2020, pp. 1672–1678, doi: 10.1109/IWCMC48107.2020.9148345.

[10] J. V. Botello, A. P. Mesa, F. A. Rodríguez, D. Díaz-López, P. Nespoli, and F. G. Mármol, "BlockSIEM: Protecting smart city services through a blockchain-based and distributed SIEM," *Sensors*, vol. 20, no. 16, p. 4636, Aug. 2020, doi: 10.3390/s20164636.

[11] Y. T. Aklilu and J. Ding, "Survey on blockchain for smart grid management, control, and operation," *Energies*, vol. 15, no. 1, p. 193, Dec. 2021, doi: 10.3390/en15010193.

[12] P. Zheng, Z. Zheng, J. Wu, and H.-N. Dai, "XBlock-ETH: Extracting and exploring blockchain data from Ethereum," *IEEE Open J. Comput. Soc.*, vol. 1, pp. 95–106, 2020, doi: 10.1109/OJCS.2020.2990458.

[13] W. T. Scherer, S. Adams, and P. A. Beling, "On the practical art of state definitions for Markov decision process construction," *IEEE Access*, vol. 6, pp. 21115–21128, 2018, doi: 10.1109/ACCESS.2018.2819940.

[14] A. Gopstein, C. Nguyen, C. O. Fallon, D. Wollman, and N. Hasting, "NIST framework and roadmap for smart grid interoperability standards release 4.0," U.S Dept. Commerce, Nat. Inst. Standards Technol. (NIST), NIST Special Publication 1108r4, Tech. Rep., 2020.

[15] Z. Pourmirza and A. Srivastava, "Cybersecurity analysis for the communication protocol in smart grids," in *Proc. IEEE 8th Int. Conf. Smart Energy Grid Eng. (SEGE)*, Aug. 2020, pp. 58–63.

[16] I. S. Stoyanov, T. B. Iliev, G. Y. Mihaylov, B. I. Evstatiev, and S. A. Sokolov, "Analysis of the cybersecurity threats in smart grid," in *Proc. IEEE 24th Int. Symp. Design Technol. Electron. Packag.*, 2018, pp. 90–93.

[17] P. Ganguly, M. Nasipuri, and S. Dutta, "Challenges of the existing security measures deployed in the smart grid framework," in *Proc. IEEE 7th Int. Conf. Smart Energy Grid Eng. (SEGE)*, Aug. 2019, pp. 1–5.

[18] Drd. I. Ionita, "Cybersecurity concerns on real time monitoring in electrical transmission and distribution systems (SMART GRIDS)," in *Proc. 54th Int. Universities Power Eng. Conf. (UPEC)*, Sep. 2019, pp. 1–4.

[19] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, "Cyber-security in smart grid: Survey and challenges," *Comput. Electr. Eng.*, vol. 67, pp. 469–482, Apr. 2018.

[20] M. Fanlin and Y. Wei, "Summary of research on security and privacy of smart grid," in *Proc. Int. Conf. Comput. Commun. Netw. Secur. (CCNS)*, Aug. 2020, pp. 39–42.

[21] A. A. Ayrancı and H. İlhan, "Decentral smart grid control system stability analysis using machine learning," in *Proc. 2nd Int. Conf. Comput. Mach. Intell. (ICMI)*, Jul. 2022, pp. 1–5.

[22] Q. Guo, S. Chen, J. Wang, and X. Pan, "Research and design of electric power engineering project management system bsed on blockchain technology," in *Proc. Int. Conf. Blockchain Technol. Inf. Secur. (ICBCTIS)*, Jul. 2022.

[23] A. S. Musleh, G. Chen, Z. Y. Dong, C. Wang, and S. Chen, "Vulnerabilities, threats, and impacts of false data injection attacks in smart grids: An overview," in *Proc. Int. Conf. Smart Grids Energy Syst. (SGES)*, Nov. 2020, pp. 77–82.

[24] Z. E. Mrabet, M. Ezzari, H. Elghazi, and B. A. E. Majd, "Deep learning-based intrusion detection system for advanced metering infrastructure," in *Proc. 2nd Int. Conf. Netw., Inf. Syst. Secur.*, Mar. 2019, pp. 1–7.

[25] Z. E. Mrabet, H. E. Ghazi, and N. Kaabouch, "A performance comparison of data mining algorithms based intrusion detection system for smart grid," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT)*, May 2019, pp. 298–303.

[26] W. F. Fihri, H. E. Ghazi, B. A. E. Majd, and F. E. Bouanani, "A machine learning approach for backoff manipulation attack detection in cognitive radio," *IEEE Access*, vol. 8, pp. 227349–227359, 2020, doi: 10.1109/ACCESS.2020.3046637.

[27] A. A. Khan, A. A. Laghari, M. Rashid, H. Li, A. R. Javed, and T. R. Gadekallu, "Artificial intelligence and blockchain technology for secure smart grid and power distribution automation: A state-of-the-art review," *Sustain. Energy Technol. Assessments*, vol. 57, Jun. 2023, Art. no. 103282.

[28] T. Mazhar, H. M. Irfan, S. Khan, I. Haq, I. Ullah, M. Iqbal, and H. Hamam, "Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods," *Future Internet*, vol. 15, no. 2, p. 83, Feb. 2023, doi: 10.3390/fi15020083.

[29] M. Kandasamy, S. Anto, K. Baranitharan, R. Rastogi, G. Satwik, and A. Sampathkumar, "Smart grid security based on blockchain with industrial fault detection using wireless sensor network and deep learning techniques," *J. Sensors*, vol. 2023, pp. 1–13, May 2023, doi: 10.1155/2023/3806121.

[30] R. Gupta, N. K. Jadav, A. Nair, S. Tanwar, and H. Shahinzadeh, "Blockchain and AI-based secure onion routing framework for data dissemination in IoT environment underlying 6G networks," in *Proc. 6th Int. Conf. Smart Cities, Internet Things Appl. (SCIoT)*, Sep. 2022, pp. 1–6, doi: 10.1109/SCIoT56583.2022.9953671.

[31] H. Shahinzadeh, S. M. Zanjani, J. Moradi, M. Fayaz-Dastgerdi, W. Yaïci, and M. Benbouzid, "The transition toward merging big data analytics, IoT, and artificial intelligence with blockchain in transactive energy markets," in *Proc. Global Energy Conf.*, 2022, pp. 241–246, doi: 10.1109/GEC55014.2022.9986604.

[32] T. Mazhar, H. M. Irfan, I. Haq, I. Ullah, M. Ashraf, T. A. Shloul, Y. Y. Ghadi, and D. H. Elkamchouchi, "Analysis of challenges and solutions of IoT in smart grids using AI and machine learning techniques: A review," *Electronics*, vol. 12, no. 1, p. 242, Jan. 2023, doi: 10.3390/electronics12010242.

[33] I. Hammouti, A. Addaim, and Z. Guennoun, "Proposed architecture of cyber security in smart grids, blockchain as solution," in *Proc. IEEE Inf. Technol. Smart Ind. Syst. (ITSIS)*, Paris, France, Jul. 2022, pp. 1–4, doi: 10.1109/ITSIS56166.2022.10118374.

[34] G. Chen, M. He, J. Gao, C. Liu, Y. Yin, and Q. Li, "Blockchain-based cyber security and advanced distribution in smart grid," in *Proc. IEEE 4th Int. Conf. Electron. Technol. (ICET)*, Chengdu, China, May 2021, pp. 1077–1080, doi: 10.1109/ICET51757.2021.9451130.

[35] A. S. Sani, D. Yuan, and Z. Y. Dong, "SDAG: Blockchain-enabled model for secure data awareness in smart grids," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Washington, DC, USA, Jan. 2023, pp. 1–5, doi: 10.1109/ISGT51731.2023.10066338.

[36] S. Samy, M. Azab, and M. Rizk, "Towards a secured blockchain-based smart grid," in *Proc. IEEE 11th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2021, pp. 1066–1069, doi: 10.1109/CCWC51732.2021.9376089.

[37] E. Esenogho, K. Djouani, and A. M. Kurien, "Integrating artificial intelligence Internet of Things and 5G for next-generation smartgrid: A survey of trends challenges and prospect," *IEEE Access*, vol. 10, pp. 4794–4831, 2022, doi: 10.1109/ACCESS.2022.3140595.

[38] E. Ebenezer, T. Swart, and T. Shongwe, "Leveraging on the cognitive radio channel aggregation strategy for next generation utility networks," *Energies*, vol. 12, no. 14, p. 2753, Jul. 2019.

[39] V. O. Nyangaresi, Z. A. Abduljabbar, S. H. A. Refish, M. A. A. Sibahee, E. W. Abood, and S. Lu, "Anonymous key agreement and mutual authentication protocol for smart grids," in *Cognitive Radio Oriented Wireless Networks and Wireless Internet* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 427. Cham, Switzerland: Springer, 2022.

[40] V. O. Nyangaresi, Z. A. Abduljabbar, M. A. A. Sibahee, E. W. Abood, and I. Q. Abduljaleel, "Dynamic ephemeral and session key generation protocol for next generation smart grids," in *Ad Hoc Networks and Tools for IT* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 428, W. Bao, X. Yuan, L. Gao, T. H. Luan, and D. B. J. Choi, Eds. Cham, Switzerland: Springer, 2022.

[41] I. Aziz, H. Jin, I. Abdulqadder, Z. Hussien, Z. Abduljabbar, and F. Flaih, "A lightweight scheme to authenticate and secure the communication in smart grids," *Appl. Sci.*, vol. 8, no. 9, p. 1508, Sep. 2018, doi: 10.3390/app8091508.

[42] Z. A. Hussien, H. A. Abdulmalik, M. A. Hussain, V. O. Nyangaresi, J. Ma, Z. A. Abduljabbar, and I. Q. Abduljaleel, "Lightweight integrity preserving scheme for secure data exchange in cloud-based IoT systems," *Appl. Sci.*, vol. 13, no. 2, p. 691, Jan. 2023, doi: 10.3390/app13020691.

[43] M. A. Al Sibahee, S. Lu, Z. A. Abduljabbar, X. Liu, H. B. Abdalla, M. A. Hussain, Z. A. Hussien, and M. J. Jassim Ghrabat, "Lightweight secure message delivery for E2E S2S communication in the IoT-cloud system," *IEEE Access*, vol. 8, pp. 218331–218347, 2020, doi: 10.1109/ACCESS.2020.3041809.

[44] S. M. Umran, S. Lu, Z. A. Abduljabbar, and X. Tang, "A blockchain-based architecture for securing industrial IoTs data in electric smart grid," *Comput., Mater. Continua*, vol. 74, no. 3, pp. 5389–5416, 2023.

NABIL TAZI CHIBI was born in Casablanca, Morocco, in 1977. He received the Engineering degree in computer science and telecommunication from the National School of Computer Science and Systems Analysis (ENSIAS), Rabat, Morocco. He is currently pursuing the Ph.D. degree with the Communications Systems Department, National Institute of Posts and Telecommunications (INPT), Morocco. He is also the Director of the Information Systems. His research interests include machine learning, blockchain, cybersecurity, and smart grids.

OMAR AIT OUALHAJ received the M.S. degree in computer science and telecommunication from the Faculty of Sciences, Mohammed V University, Rabat, Morocco, in 2012, and the Ph.D. degree in computer science from the National School of Computer Science and Systems Analysis (ENSIAS), Mohammed V University, in March 2019. He is currently a Professor Assistant with the National Institute of Posts and Telecommunications (INPT), Rabat. His research interests include the Internet of Things (IoT), sensor networks, ad-hoc networks, delay tolerant networks (DTNs), vehicular networks (routing and energy efficiency), mobility, and the performance evaluation of mobile networks using game theory and MDP, learning approach, and machine learning techniques. He is actively involved in research and continues to contribute to diverse scientific communities. He served as a Reviewer for numerous renowned international journals and conferences, such as TNSESI, IEEE GLOBECOM, IEEE ICC, IEEE WCNC, *ICT Express*, and IWCMC.

WASSIM FASSI FIHRI received the M.Sc. degree in computer science and telecommunications from Ibn Tofail University, Morocco, in 2008, and the Ph.D. degree in computer science and telecommunications from Institut National des Postes et Télécommunications (INPT), Morocco, in 2021. He is currently a Cybersecurity Architect and a certified Project Manager Professional (PMP). His research interests include cybersecurity, networking, cognitive radio networks, machine learning, and blockchain. He is the author of more than six publications in renowned conferences and journals, such as IEEE Access, Springer, and Wiley.

HASSAN EL GHAZI received the M.S. degree in wireless communications and the Ph.D. degree in electrical engineering from Université Polytechnique Hauts-de-France, France, in 2004 and 2008, respectively. He is currently an Associate Professor with the Communications Systems Department, National Institute of Posts and Telecommunications (INPT), Morocco. He advised many Ph.D. and graduate students at both INPT and Mohammed V University, Rabat, Morocco. So far, his research contributions have culminated in more than 50 papers in a wide variety of international journals and conferences. His research interests include cyber-physical security, smart grid systems, and cognitive radio networks. He served as a Reviewer for IEEE Access, Elsevier, and Springer. He served as the General Chair for the IWTSC'18 Conference and the Conference Chair for the NISS'19 Conference.