IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 4 June 2023, accepted 9 July 2023, date of publication 18 July 2023, date of current version 27 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3296482

RESEARCH ARTICLE

A Blockchain-Based Architecture and Framework for Cybersecure Smart Cities

ABLA EL BEKKALI[1,2], MOHAMED ESSAAIDI[1], (Senior Member, IEEE), AND MOHAMMED BOULMALF[2]

[1]Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes (ENSIAS), Mohammed V University, Rabat 10000, Morocco
[2]International University of Rabat, Rabat 11100, Morocco

Corresponding author: Abla El Bekkali (abla.elbekkali@um5s.net.ma)

ABSTRACT A smart city is one that uses digital technologies and other means to improve the quality of life of its citizens and reduce the cost of municipal services. Smart cities primarily use IoT to collect and analyze data to interact directly with the city's infrastructure and monitor city assets and community developments in real time to improve operational efficiency and proactively respond to potential problems and challenges. Today, cybersecurity is considered one of the main challenges facing smart cities. Over the past few years, the cybersecurity research community has devoted a great deal of attention to this challenge. Among the various technologies being considered to meet this challenge, Blockchain is emerging as a solution offering the data security and confidentiality essential for strengthening the security of smart cities. In this paper, we propose a comprehensive framework and architecture based on Blockchain, big data and artificial intelligence to improve smart cities cybersecurity. To illustrate the proposed framework in detail, we present simulation results accompanied by analyses and tests. These simulations were carried out on a smart grid dataset from the UCI Machine Learning Repository. The results convincingly demonstrate the potential and effectiveness of the proposed framework for addressing cybersecurity challenges in smart cities. These results reinforce the relevance and applicability of the framework in a real-world context.

INDEX TERMS Smart city, smart grid, cybersecurity, framework, IoT, blockchain, big data, artificial intelligence.

I. INTRODUCTION

In the digital age, everything is connected as part of the growing and accelerating digital transformation of modern societies, which involves all kinds of sectors and human activities such as education, healthcare, economy, energy, etc. Urban communities, and even some villages, are benefiting from the technologies and solutions available through digital transformation to engage in all kinds of smart city initiatives to put them at the service of sustainable, resilient and inclusive socio-economic development. The smart city achieves efficiencies, promotes sustainability, and improves the quality of life for its residents through the integration of technology. Planning for a smart city is essentially about bringing the Internet of Things (IoT) to scale. The Internet of Things (IoT) is the network of physical terminals, objects, incorporating software, connectivity, sensors, etc., to connect to other systems on the internet and exchange data to provide proper management and monitoring of city infrastructure and operations. Driven by the growing urban population, IoT and ICT are the main pillars of smart cities to improve their efficiency as well as the lives of their citizens [1], [2]. A smart city needs technological efficiency in areas as diverse as transportation and mobility, services, communication, security, citizen relations, etc. The implementation of IoT-based applications within cities allows for the optimization of: energy control, building performance, street furniture management, waste disposal, mobility, etc. The beneficiaries are citizens, consumers, private companies and local authorities [3]. By offering increasingly digitized services, smart cities are becoming ever more connected but also more exposed to cyber risks and cyber-attacks. Data collection is

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

essential in IoT-based applications and services that are considered key assets for monitoring and operating smart cities. Therefore, managing data across the smart city infrastructure is a big challenge given all the connected devices involved and their different architectures and urban data must be protected throughout its lifecycle. However, the main challenge is to protect IoT infrastructures throughout their deployment [4]. In this case, an important question arises, namely: how to transfer all data quickly, securely and without third-party intermediaries?

The use of the Blockchain within Smart Cities would allow a more controlled governance by reappropriating personal data that would no longer be controlled by intermediaries. It offers the possibility of encrypting and securing the information transmitted while ensuring its traceability and maintaining its anonymity. In addition, it optimizes the interconnection of all the services offered in the city but also provides real-time information on mobility (e.g., vehicles used, routes taken, etc.), energy, waste management, etc., [5], [6]. The blockchain is a distributed system based on a sequence of blocks allowing the storage and transmission of information. One of the advantages of blockchain technology is the traceability of all transactions, as well as its operation without a central controlling authority, which makes it decentralized, secure and transparent. Cryptography helps users to validate information, thus ensuring its authenticity [7]. The members chosen in the blockchain to manage the technical structure of the implementation are paid for their role in checking, verifying and validating the consistency with other information in the blockchain. Once verified and validated the block is time-stamped and added to the blockchain. Everyone can then view and access this information, but not modify it. In case of an error, it will be corrected by a new transaction [8]. Smart contracts present a computer equivalent of the paper contract, they are usually deployed on a blockchain and refer to irrevocable computer programs that execute specific instructions that must be followed. During the execution of the smart contract, all verification steps are recorded in the blockchain used, a process that prevents modification or deletion after the fact, thus protecting and securing all data [9].

Artificial intelligence (AI) enables machines to replicate human cognitive abilities such as reasoning, language, perception, etc. It also refers to the ability of computers and robots to perform intelligent tasks without requiring human intervention. With machine learning (ML) methods, AI analyzes data to organize information and learn to solve problems, but in rule-based or logic-based systems, problem solving is programmed by humans. Both AI and blockchain are being leveraged to build smart cities based on data-intensive applications. As a result, they can help smart cities achieve "data sovereignty" and improve data security, with traceable and secure transactions, preventing situations such as misuse cases and data leakage [10]. Among the ML libraries, Spark's Mllib has succeeded in making ML simple and scalable. It is a machine learning library that enables high-speed, high-quality analysis of algorithms.

The various tools it provides are: ML algorithms that include classic machine learning algorithms such as regression, classification, collaborative filtering and clustering. Characterization which includes feature extraction, transformation, dimensionality reduction and feature selection. Pipelines, which allows for the evaluation, construction and tuning of ML pipelines. Persistence, which offers saving, loading of algorithms, models and pipelines to reduce time and effort. Also, utilities such as data processing, statistics, linear algebra, etc.

Smart cities IoT platforms collect, process and distribute data in large quantities. Such massive data streams require another level of computing power to be analyzed and processed in real time. Today, the focus should be on making better use of existing infrastructure and data. The massive volume of data generated by smart cities requires that it be collected, managed, and analyzed to provide useful information, functionality and insight. This presents cities with a new challenge: controlling, moving, and restoring their data anytime, anywhere [11], [12].

Moreover, there are thousands of IoT devices in smart cities which interact with each other and implement complex applications [13]. However, the use of Big Data could improve the services they provide in different areas. AI algorithms such as machine learning play an important role in Big Data analysis and present accurate analysis of real-time data. However, designing and implementing AI and ML-based Big Data analytics has inherent challenges in terms of data security, privacy and centralized architecture. Integrating blockchain technology into smart cities is essential to overcome these challenges. Hence, by integrating these technologies, we could overcome these challenges and provide an effective solution for cyber-secure smart cities. Therefore, the proposed research mainly presents a blockchain-based cybersecurity approach for smart cities while covering other topics on how data collected by IoT devices should be managed using big data and AI techniques and approaches.

This paper presents in its second section an in-depth analysis of Blockchain technologies and approaches, namely the types, consensus protocols and its benefits for smart cities. Section III presents a literature review of recent cybersecurity-related blockchain-based solutions for smart cities, with their benefits and limitations. Section IV is dedicated to the presentation of our proposed solution including the architecture, data flow diagram, data dictionary, and results obtained from the deployment and testing performed. The last section of the paper presents the conclusions of the proposed research work.

II. BLOCKCHAIN

A. BACKGROUND

Blockchain is a technology that is gaining enormous momentum for different applications and is compared to a necklace, each bead of which is a record of an action, and the chain cannot be broken. The blockchain is therefore an indestructible digital record of actions. This technology revolutionizes the means by which we transmit our data using cryptography according to an ethical philosophy. It offers a decentralized, secure and transparent database, allowing the transfer of values, goods, messages, and any type of data. It allows creating a database whose authenticity can be verified by the community. Digital assets are distributed assets allowing the creation of an immutable record of an asset, and also decentralized allowing real-time access and transparency to the public. Blockchain will become a decentralized global source of trust and a technology of choice for everyone [14], [15].

The blockchain consists of 3 key elements namely:

Blocks which are presented by transactions. According to the amount of data they contain, these blocks are distinguished by an identifier which is a unique and specific code called ''hash''. The second element is the nodes that represent the computers connected to the blockchain, which host a copy of the database that is downloaded automatically when connecting to the network and which includes and allows all exchanges between users. The last element is the miners who have an essential role within the blockchain which is to verify if the new blocks created correspond to the security standards. These miners thus make it possible to guarantee the authenticity of the blocks, and thus of the whole chain.

B. TYPES OF BLOCKCHAIN

There is not one blockchain technology, but hundreds, with variations that are sometimes very technical, often commercial. These technologies are classified as follows:

Private Blockchain: A private or permissioned blockchain is an implementation of a technology in which a person must give permission to access it. A private blockchain is totally centralized, for which the term ''permitted'' is used. The management of the infrastructure, its management rules and its operation are fully centralized. It allows information to be exchanged between different partners. The information entered is time-stamped and signed. This makes it possible to ensure that information has indeed been exchanged at a given date and time, and its author is identifiable. The level of security is natively high, the exchanges are encrypted and the actors are known by name. Failing this, a correspondence table is available to the administrator to make a correspondence between an alias and a natural person [16].

Consortium Blockchain: It has both private and public blockchain characteristics. It is shared between different actors having an interest in collaborating together. Block validation decisions are made by a majority of the largest members rather than by the network as a whole. Decision makers can make some information public. The consortium blockchain tends to be more secure, scalable and efficient than a public blockchain network. Access to this blockchain is less centralized, as access authorization is typically done through an authority for each participating company [17]. The function of this authority is to manage access in a delegated manner. The actors are therefore known and an alias logic is strongly recommended to identify them [18].

Public Blockchain: or permission-less blockchain allows to carry out transactions that will be recorded and validated by the entire network. Everyone can write and read without going through a central regulatory authority. This is why it is called a non-permissioned solution [19]. This can be compared to an unfalsifiable register kept by all its

TABLE 1. Analysis of different types of blockchain.

TYPE	Private Blockchain	Consortium Blockchain	Public Blockchain
Nature	Permissioned Open to an individual or an entity	Semi-decentralized Open to specific organizations and groups	Permissionless Completely open
Participant	Identified Trusted	Identified Trusted	Anonymous Could be malicious
Consensus protocols	pBFT RAFT	pBFT	PoW PoS DPoS
Energy consumption	Low	Low	High
Transaction speed	Extremly fast	Fast	Slow
Transaction Cost	Not so costly	Low cost	Costly
Transparency	Only transparent to the users who are granted access	Better transparency	Completely transparent
Scalability	High	Low	High
Efficiency	High	High	Low
Example	Hyperledger, Ripple, R3	Blockchain, Blockstack, Multichain	Ethereum, Blockstream, Bitcoin, Litecoin, Dash, Factom

actors. Verification of transactions and validation of blocks is done by these actors who are called miners. This guarantees the continuous updating of data, reliability and security, and in crypto-assets they are rewarded for this work. This blockchain works in peer-to-peer, it is a decentralized network which consists, thanks to a relationship of trust, in making an exchange between two actors without an intermediary. It offers everyone the possibility to make transactions and verify them, which allows it to be freely accessible. These transactions are pseudonymous and not anonymous. The identities of people are not recorded in the blockchain. On the other hand, it is possible to find the identity of a person via his/her public address [20], [21].

Table 1 illustrates a comparison among the three types of Blockchain according to different criteria, namely, nature, participant, consensus protocol, energy consumption, transaction speed, transaction cost, transparency, scalability, and efficiency.

C. CONSENSUS PROTOCOLS

Are considered one of the most revolutionary and important aspects of the Blockchain. Blockchain consensus protocols create a system of irrefutable agreement between different parties within a distributed network, while preventing malicious exploitation of the system [22]. Blockchain consensus protocols ensure synchronization among all network nodes. Each consensus aims to answer a specific question, namely, how can the authenticity of each transaction be ensured? Any individual can submit information and decide to store it on a blockchain. It is therefore essential to be able to review this information and decide by consensus whether or not it is possible to add it to the network. The term ''consensus'' means that all nodes in the network must agree on an identical version of the blockchain [23]. Somehow, the consensus mechanism of a blockchain is an internal and automatic audit of its network, and this in two functions, namely:

- It allows to update the blockchain while ensuring the validation of each block. People participating in block validation (referred to as network ''nodes'') must have an incentive to engage in network security.
- Prevents the control of the whole network by a single entity and thus guarantees its decentralization.

The main consensus protocols are:

Proof-of-Work (PoW): The Proof-of-Work protocol is the most widely used of all blockchain consensuses. Since 2009, it has been able to demonstrate its resistance and security to various attempted attacks. In the Proof-of-Work protocol, the different network nodes are called miners. Miners solve a complex mathematical problem with significant computing power to confirm a transaction. So, they use a mathematical process called a hash function. Hash allows transaction data to be written in blocks and connected to each other. There are different types, such as SHA 256, used on Bitcoin. Once the hash is entered in the blockchain, it cannot be falsified. A miner is rewarded for each block he manages to approve and confirm. Its reward / income is proportional to the computing power it is able to deploy to solve the problem [24].

Proof of Stake (PoS): This is a much simpler and cheaper process, where the process of committing the transaction is called ''forging'' and the actors involve their own set of nodes. Validators are rewarded for their efforts: the higher the stakes, the better the chances of validation and the higher the returns. PoS also involves a process called ''sharding'' which involves horizontal partitioning of nodes and improves the scalability of the process. PoS does not involve mining and therefore no complicated puzzle solving. Therefore, there is no need to continually update the software and the power consumption is weak. Furthermore, the forging process is much cheaper than mining, PoS is completely decentralized and not all nodes need to be involved in the system [25], [26].

Delegated Proof of Stake (DPoS): It offers a hybrid model to address the weaknesses of PoW and PoS. Like PoS it works based on the same basic principle. It is up to the members of the community to elect the people who will be responsible for forging the blocks. The elections system ensures that the blockchain is not controlled by a minority of people, such as a miner with a lot of computing power, or a PoS counterfeiter with a very large amount of tokens [27].

Proof of Burn (PoB): PoB is a consensus mechanism used to validate new blocks on a blockchain. This mechanism is based on the destruction of tokens by participants. Only those who can prove that they have destroyed a predetermined amount of coins are deemed trustworthy enough to support the validation of a new block [28].

Proof of Elapsed Time (PoET): Used primarily in permissioned blockchains like Hyperledger Sawtooth (in addition to pBFT). Like a lottery it uses random selection to choose which node will win the new block. ''Miners'' must obtain a membership certificate to join the network. Once in the network, a time is randomly decided, which the nodes must wait. The miner must wait the minimum defined time before starting to mine a new block in the blockchain. The miner with the shortest wait time is elected to mine the block that round. The system tends to be fair and select miners with a good degree of randomness [29].

Proof of Capacity (PoC): Proof of space or proof of storage, it is an alternative to proof of work which is based, not on the energy expenditure of the validating machines, but on their ability to keep data memory. It allows these participants to decide on mining rights and validate transactions in the blockchain via the space available on the hard drive of their computer. The creation of this system contrasts with the use of the computing processing power of equipment necessary for mining as well as the participation of the validator in cryptocurrencies. Proof of capacity is used on blockchains to manage the validation of new blocks. The participants of this consensus temporarily provide the storage space of their hard drives as a stake [30]. The mechanism is considered to be extremely energy and

TABLE 2. **An analysis of the main blockchain consensus protocols.**

Consensus Protocols	PoW	PoS	DPoS	PoB	PoET	PoC	pBFT	PoA
Programming Language	Solidity, C++, Golang	Solidity, Scala, C++	C++, Javascript	Golang, C++, Solidity, Serpent	Python	Python	Python, Java, Golang	Solidity, Java
Speed	Slow	Fast	Fast	Medium	Medium	Slow	High	Low
Resource consumption	High	Low	Low	Medium	High	High	High	High
Energy Efficiency	Low	High	High	Low	High	High	High	Low

resource efficient, which makes it more accessible to a wider audience.

Practical Byzantine Fault Tolerance (pBFT): was introduced for the first time in 1999. It is a protocol that can be applied to large networks because it has the advantage of processing tens of thousands of transactions per second. The algorithm makes it possible to maintain security properties as long as less than a third of the nodes or replicas are corrupted [31].

The various steps in the basic communication model in the pBFT protocol are as follows: REQUEST where the client sends its service request to the main server. PRE-PREPARE where the main server gives this request a number and sends a PRE-PREPARE message to the other servers. PREPARE when a "PREPARE" message is sent by each server to the other servers. COMMIT when a "COMMIT" message is sent to the other servers. The last step named REPLY includes the decision when a sufficient number of servers agree on the request order, each server sends its response to the client. This consensus protocol attempts to provide a convenient Byzantine state machine replication that works even in the case where malicious nodes are present. The nodes in a pBFT-enabled distributed system are arranged in order, with one node being called the primary node and the other node being called the secondary or backup node. However, each node can become the primary node by moving from the secondary to the primary node, primarily in the event that the primary node fails. The goal here is for all honest nodes to help reach a consensus on the state of the system based on majority rule. As a result, the pBFT system works when the maximum number of malicious nodes does not exceed one-third of the total number of nodes in the system. This means that the system becomes more secure as the number of nodes increases [32].

Proof of Authority (PoA): This is a variation of the PoS consensus mechanism where, instead of tokens, network participants stake their identity and reputation. PoA, or Proof of Stake Authority (PoSA) seeks to solve the problems encountered in PoW and PoS consensus protocols [33].

We analyze and present the consensus protocols according to programming language, speed, resource consumption and energy efficiency. Table 2 below shows the results of the analysis and comparison between different consensus protocols [34], [35].

D. BLOCKCHAIN FOR SMART CITIES

The Blockchain can respond to a large number of current issues and it represents an ultra-competitive data transmission technology. The use of the Blockchain within Smarts Cities would allow a more controlled governance by the re-appropriation of personal data which would no longer be controlled by intermediaries [36]. It offers the possibility of encrypting, securing and traceability of data transmitted while maintaining anonymity. Moreover, it allows to optimize the interconnection of all the services offered in the Smart City and makes it possible to access real-time data on all kind of services such as mobility (vehicles used, routes taken, etc.), energy, waste management, etc., [1] [3].

In addition, Smart Cities can use blockchain technologies to reach several objectives [9]:

- Easy and secure data exchange.
- Promotion of collaboration among public administrations.
- To obtain a single view of the Smart City's supply chains.
- To reduce fraud and verify financial transactions faster.
- To create smarter and more efficient supply chains.
- To simplify processes for reconciling data disputes for audit and regulatory compliance.
- To manage energy consumption, urban development and population growth.

TABLE 3. Analysis of blockchain-based solutions for smart cities.

Ref	Description	Technologies	Benefits	Limitations
[37]	A decentralized big data auditing scheme for smart city environments with Blockchain capabilities called Data Auditing Blockchain (DAB).	Blockchain Big Data	- Provides the ability to trace all audit history and allow all data files to be audited by any data owner or user at any time. - Avoid centralized dependency.	Not implement.
[38]	An MEC-based sharing economy system, relying on an AI infrastructure, Blockchain and off-chain framework to store immutable ledgers.	Blockchain AI Big data	- A sustainable incentive mechanism for secure smart city services.	Implementing large-scale tests in shared economy scenarios has one major limitation: the difficulty of faithfully reproducing real-life conditions, collecting and analyzing data, and taking into account all the external factors that can influence test results.
[39]	A system in which vehicles that belong to the fleet can be part of a single ITS network that provides services to all autonomous vehicles while performing their normal work.	Blockchain AI	- Mutual trust data sharing architecture using Blockchain technology and AI to operate mobile operators.	In terms of contribution, there is a perceived deficit from the companies' point of view.
[40]	Propose a sustainable automotive ecosystem.	Blockchain AI	- A mobility solution. - Security. - Automated maintenance services. - Supply chain management.	Dynamic expandability.
[41]	A secureSVM for smart cities that is Blockchain-based which allows collected IoT data to be encrypted and stored on a distributed ledger.	Blockchain AI	- Preserving SVM-ML privacy.	Resource consumption.

III. RELATED WORKS

Table 3 summarizes various approaches using Blockchain technology to solve several cybersecurity issues in smart cities. Our aim is to highlight the advantages as well as the inherent limitations of these approaches, offering a more accurate and relevant overview of the situation.

IV. PROPOSED SOLUTION

A. ARCHITECTURE

In this section, we present the architecture of our solution that focuses mainly on security in smart cities using blockchain.

For the deployment of our solution, we use Docker which is an open-source and secure containerization software platform designed for the creation, deployment, and management of virtualized applications. Knowing that traditional virtualization methods based on virtual machines have certain limitations, the container is a better alternative that guarantees a lightweight and simpler execution environment.

The architecture we propose is based on three layers: the perception layer, the data processing layer and the blockchain layer (Figure 1).

Perception layer: In the perception layer, the objective is to collect, process and send data to the next layer. This layer includes various applications and domains of smart cities such as (environment, mobility, government, economy, people, life). This layer consists of sensors and IoT devices to collect data, as well as Big Data real-time query components to ingest this data, API connectors and REST APIs that will enable web requests. In this layer, IoT data is sent to a data cube, then this data is aggregated to calculate key performance indicators and then it will be sent to the next layer.

Data processing layer: In this layer, we integrate machine learning. Preprocessing of data using machine learning is done because the collected data is in a raw format and it is not always possible to train/test the model using it. It is important to process this raw data in order to interpret it correctly and avoid any negative results in the prediction. In our case, we are dealing with too massive databases, which makes the computations too slow. We then decided to use PySpark DataFrame [10] which is one of the most optimized Machine Learning platforms for dealing with massive databases using distributed programming, and which consists of using multiple distributed computing units on multiple nodes to reduce the execution time of a query. Our algorithm uses the historical data of the Blockchain to build the model (training and testing), thus, after the end of the preprocessing and through PySpark the historical data of the Blockchain will be read in order to train/test the model, then, we use the linear regression model to predict the new records of the variable "stab", this prediction tool solves the binary classification problem (i.e., stable or unstable). We point out that the result of the linear regression model gave a high accuracy with an Rsquared of 0.9999998832117597. This data will be sent to the next blockchain layer.

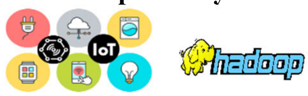
Blockchain Layer 	▪ The data will be submitted to a pBFT analysis in order to validate their integration or not in the blockchain. ▪ Ensures the security of each record by using a hash system. ▪ By integrating the pBFT consensus protocol we get the following results: -Success: The hash is valid. A new block has been added to the chain. -Success: The current hash is valid. The data already exists in the blockchain. -Failure: The hash is not valid. Please try again.
Data processing Layer 	▪ Its role is the preprocessing of the collected data. ▪ Reading historical data from the blockchain to build the model ▪ The prediction of new records "stab".
Perception Layer  	▪ Consists of IoT devices and sensors, Big Data real-time query components, API connectors and REST APIs. ▪ Its role is to collect, process and send data to the next layer.

FIGURE 1. Architecture.

Blockchain layer: This layer evaluates via the pBFT whether the data is valid and can be integrated into the blockchain or not. This layer uses a hash system that assigns a hash to each record before passing through the pBFT process that decides whether or not to integrate them into the blockchain. This data is subject to the practical application of Byzantine Fault Tolerance, this pBFT consensus protocol was chosen because it ensures energy efficiency and protects the system from failures by using collective decision making (involving both correct and malicious nodes), and thus reduces the influence of malicious nodes. The following results are obtained:

- 'Success: Hash is valid. New block was added to the chain'
- 'Success: Current hash is valid. Data already exists in the Blockchain'
- 'Failure: Hash is invalid. Please try again'

B. META DATA

This section first presents the data flow diagram which is visual representations of the data processing performed to illustrate, explain and analyze the model (Figure 2). Next, the data dictionary corresponding to the solution is presented in Table 4. The dataset chosen to illustrate the implementation of the proposed framework is based on smart grid "Electrical Grid Stability Simulated Dataset" from UCI Machine Learning Repository and contains 60,000 obser-

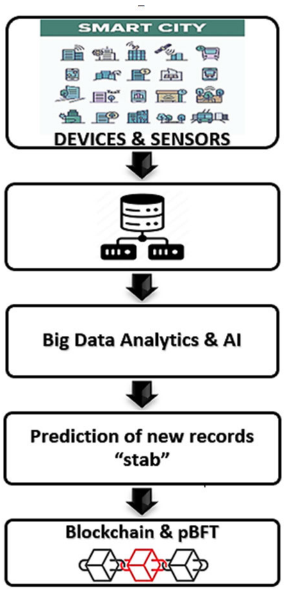


FIGURE 2. Data flow.

TABLE 4. Data dictionary.

VARIABLE NAME	TYPE/ FORMAT	VARIABLE DESCRIPTION
'tau1' to 'tau4'	NUMERIC	("tau1" corresponds to the supplier node and "tau2" to "tau4" represent consumer nodes). This is the reaction time of each participant in the network. Its value is between 0.5 and 10.
'p1' to 'p4'	NUMERIC	The nominal power by each participant in the network. If it is positive, it means that it is produced and if it is negative, it means that it is consumed.
'g1' to 'g4'	NUMERIC	The "g" stands for "gamma". It is the coefficient of price elasticity for each participant in the network. Its value is between 0.05 and 1.00.
'stab'	NUMERIC	If this variable is positive, the system is linearly unstable, if not if it is negative, the system is linearly stable.
'stabf'	STRING	It designates a categorical (binary) label. The relationship between stab and stabf (stabf = stable if stab <= 0, unstable otherwise).

vations and 14 variables [42]. A smart grid is a very important component of a Smart City that ensures resilient delivery of energy for their many functions, present opportunities for conservation, improve efficiency, and, most importantly, enable coordination between city authorities, infrastructure operators, public safety officials, and the public [43].

C. RESULTS AND DISCUSSION

For the sake of illustration of the proposed approach for smart cities cybersecurity, we will implement it to secure a smart grid based on a dataset from the UCI Machine Learning Repository [42].

The use of Docker in this approach features efficient container management, high portability and compatibility, and offers an isolated environment ensuring better security, reliability and deployment flexibility. The integration of big data using Hadoop for storage and PySpark for data processing, together with artificial intelligence, means that large quantities of data from smart cities can be analyzed and monitored in real time to detect vulnerabilities. Predictive models and machine learning algorithms are also used to identify malicious traffic patterns. The integration of blockchain offers a secure, decentralized infrastructure for authentication and data confidentiality in smart cities. It enables the creation of unique digital identities and guarantees the integrity of transactions. Also, pBFT integration offers energy efficiency, low latency, transaction finality and high throughput, it is optimized to continuously improve transaction speed and performance while guaranteeing security. In this way, it enhances the resilience of smart cities by enabling data replication and decentralized decision-making, meaning that if one node or part of the network fails, the other nodes can continue to operate autonomously and maintain the network's operability.

By synergistically combining these technologies, our approach benefits from advanced threat detection, robust authentication, proactive risk management, enhanced resilience and informed, data-driven decision-making, helping to strengthen the security of smart cities.

Figure 3 below measures the linear correlation between the variables based on Pearson's coefficient. Pearson correlation coefficient, represented by "r", is an index that measures the linear relationship between two continuous variables, see equation (1). The correlation coefficient varies between −1 and +1. A value of −1 or +1 reflects a complete correlation between the variables, while a value of 0 indicates no correlation between them. When the value is greater than 0, it indicates that the correlation is positive, which means that the variables vary together in the same direction. However, when the value is less than 0, it indicates a negative correlation between the two variables, which then means that when one variable increases, the other decreases [44]. It is important to check the correlation between each numerical variable and the base variable, as well as the correlation between numerical variables leading to potential undesirable collinearity.

$$r = \frac{\sum_{i=1}^{n}(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \bar{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i - \bar{Y})}} \tag{1}$$

The resulting r-value is an estimate of the correlation between continuous variables in smart grids in smart cities. In our case, if "stab" variable is positive, the system is linearly unstable and if it is negative, the system is linearly stable.

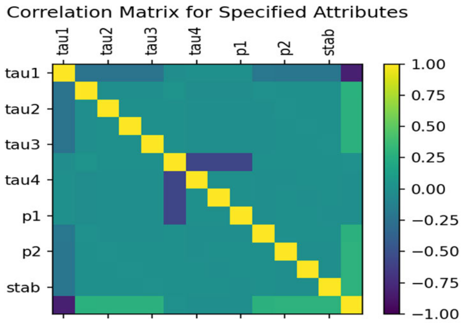


FIGURE 3. Pearson correlation for variables of the Smart Grid.

Figure 3 shows that there is no multi-colinearity, and more importantly that the predictor variables are perfectly correlated with the stab variable.

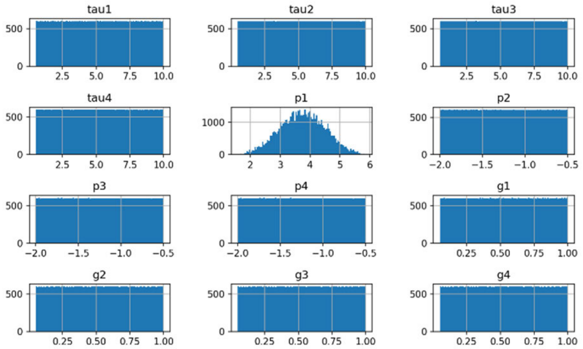


FIGURE 4. Normal distribution of the Smart Grid variables.

In Figure 4, a histogram is used to describe the normal deviation between the variables. We then graphically present the distribution patterns of the continuous quantitative variables that we have. The histogram allows for a quick inspection of the shape of the distribution. Normalization is a technique applied to the preparation of data for machine learning. It is therefore a necessary condition to check if my data follow a normal distribution or not, in order to decide if the test conditions are valid or not.

The Smart Grid dataset data used [42] comes from simulations with predetermined fixed ranges for all variables. We note that the distributions are fairly uniform, with the exception of p1 which follows a normal distribution with a very small skewness factor of -0.013.

In Figure 5, using a Box Plot we demonstrate the spread of data (normality). Box Plot is the most commonly used graphical visualization in the literature because of it is very rich of information (Min, Max, Q1, Q2, Q3, IQR). It consists of a rectangle from which two lines emerge to represent certain elements of the data [44].

- The central value of the graph is the median (there are as many values above as below this value in the sample).
- The edges of the rectangle are the quartiles (for the lower edge, one quarter of the observations have smaller values and three quarters have larger values, the upper edge follows the same reasoning).
- The ends of the whiskers are calculated using 1.5 times the interquartile range (the distance between the 1st and 3rd quartile).

Any deviation from the median of the center, presents an asymmetric distribution and therefore it is not normal.

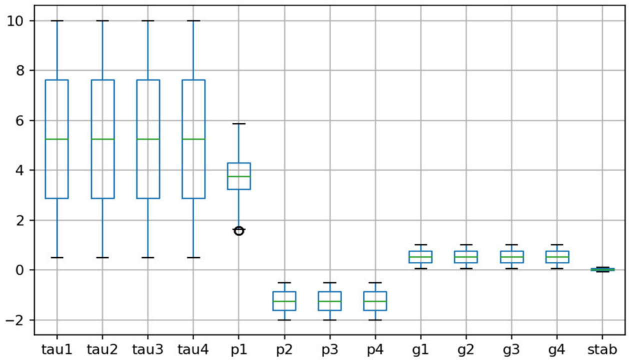
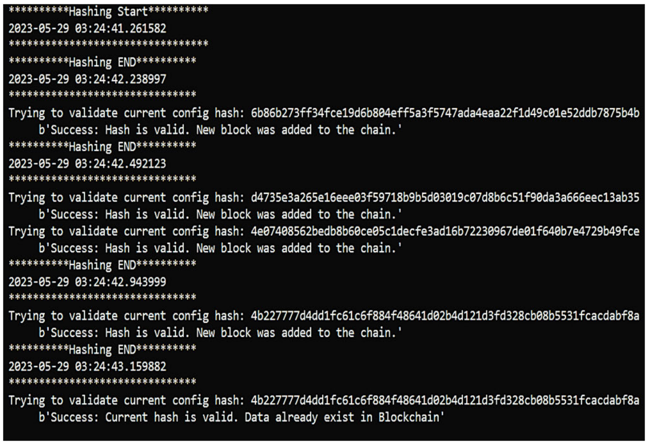


FIGURE 5. Spread of data through Boxplot.

Using the Box Plot, we can see that the values are within the norm because all observations are inside the boxes. Therefore, we can deduce that these observations have values that are not outliers.

The Blockchain offers several practical uses to strengthen security in smart grids and smart cities. It allows a more controlled governance by reappropriating personal data that would no longer be controlled by intermediaries, the possibility of encrypting and securing transmitted data by knowing their origin and destination while maintaining anonymity, and optimizing the interconnection of all services offered in the smart city [45] (i.e. smart city verticals). What the Blockchain brings is a more accurate examination based on the validity of the connection information, and the possibility of preventing the data or the computer system itself from being subject to attempts to modify it. From our analysis of the different consensus protocols presented in Table 2, we found that pBFT is the most effective and proven one. Indeed, unlike other protocols, pBFT offers better performance and provides security, liveliness and decentralization properties.

In Figure 6, shows the reliability and efficiency of our model and of the Blockchain layer by performing a few interactions with it. This is based on a test consisting to create a new dataset based on the 14 existing variables of the original dataset. We insert 4 rows of data and duplicate the last one to simulate duplicate data. This test allows us to check that the model is working properly and to evaluate its ability to handle realistic situations.

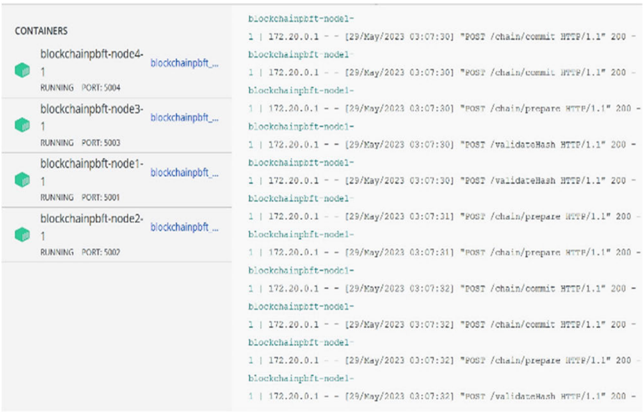


```
**********Hashing Start**********
2023-05-29 03:24:41.261582
********************************
**********Hashing END**********
2023-05-29 03:24:42.238997
*******************************
Trying to validate current config hash: 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
     b'Success: Hash is valid. New block was added to the chain.'
**********Hashing END**********
2023-05-29 03:24:42.492123
*******************************
Trying to validate current config hash: d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
     b'Success: Hash is valid. New block was added to the chain.'
Trying to validate current config hash: 4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fce
     b'Success: Hash is valid. New block was added to the chain.'
**********Hashing END**********
2023-05-29 03:24:42.943999
*******************************
Trying to validate current config hash: 4b227777d4dd1fc61c6f884f48641d02b4d121d3fd328cb08b5531fcacdabf8a
     b'Success: Hash is valid. New block was added to the chain.'
**********Hashing END**********
2023-05-29 03:24:43.159882
*******************************
Trying to validate current config hash: 4b227777d4dd1fc61c6f884f48641d02b4d121d3fd328cb08b5531fcacdabf8a
     b'Success: Current hash is valid. Data already exist in Blockchain'
```

FIGURE 6. Blockchain test results.

From the Blockchain interaction test results, we obtain 4 valid hashes meaning that new blocks have been added to the chain, and one valid hash with existing data. Hence, we can deduce the regularity of the proposed model and the applicability of pBFT to constrained IoT devices exchanging intensive secure data between nodes to guarantee network integrity.

Figure 7 shows the status of the IoT nodes in the docker, as well as an overview of the logs showing the different pbft steps.



CONTAINERS

blockchainpbft-node4-1 blockchainpbft_...
RUNNING PORT: 5004

blockchainpbft-node3-1 blockchainpbft_...
RUNNING PORT: 5003

blockchainpbft-node1-1 blockchainpbft_...
RUNNING PORT: 5001

blockchainpbft-node2-1 blockchainpbft_...
RUNNING PORT: 5002

```
blockchainpbft-node1-
1 | 172.20.0.1 - - [29/May/2023 03:07:30] "POST /chain/commit HTTP/1.1" 200 -
blockchainpbft-node1-
1 | 172.20.0.1 - - [29/May/2023 03:07:30] "POST /chain/commit HTTP/1.1" 200 -
blockchainpbft-node1-
1 | 172.20.0.1 - - [29/May/2023 03:07:30] "POST /chain/prepare HTTP/1.1" 200 -
blockchainpbft-node1-
1 | 172.20.0.1 - - [29/May/2023 03:07:30] "POST /validateHash HTTP/1.1" 200 -
blockchainpbft-node1-
1 | 172.20.0.1 - - [29/May/2023 03:07:30] "POST /validateHash HTTP/1.1" 200 -
blockchainpbft-node1-
1 | 172.20.0.1 - - [29/May/2023 03:07:31] "POST /chain/prepare HTTP/1.1" 200 -
blockchainpbft-node1-
1 | 172.20.0.1 - - [29/May/2023 03:07:31] "POST /chain/prepare HTTP/1.1" 200 -
blockchainpbft-node1-
1 | 172.20.0.1 - - [29/May/2023 03:07:32] "POST /chain/commit HTTP/1.1" 200 -
blockchainpbft-node1-
1 | 172.20.0.1 - - [29/May/2023 03:07:32] "POST /chain/commit HTTP/1.1" 200 -
blockchainpbft-node1-
1 | 172.20.0.1 - - [29/May/2023 03:07:32] "POST /chain/prepare HTTP/1.1" 200 -
blockchainpbft-node1-
1 | 172.20.0.1 - - [29/May/2023 03:07:32] "POST /validateHash HTTP/1.1" 200 -
```

FIGURE 7. IoT nodes in the Docker.

All these results show clearly the potential of the proposed approach for smart cities cybersecurity.

TABLE 5. A benchmark of our approach with main approaches from the literature.

Ref	Advantages	Strengths of our approach
[37]	- Audit and Traceability - Decentralization	- Improved auditing and traceability: Compared to this approach, which has not been implemented, our solution incorporates the PBFT protocol, which allows all transactions to be recorded in the blockchain, ensuring that they remain unchanged. The integration of artificial intelligence and Big Data capabilities makes it possible to examine this information and identify potential errors (Figure 3,4,5). In this way, every piece of data can be traced at any time, offering a more reliable auditing process. Furthermore, using Docker enables resources to be isolated, meaning that each component of the solution runs in a separate container to limit interactions between them. In addition, it offers integrated functionality for capturing and managing container execution logs (Figure 7), enabling actions to be traced, errors to be detected and security audits to be carried out. - Reinforced decentralization: Using Docker reinforces the principle of decentralization by offering container portability, which facilitates consistent distribution of services across different nodes, efficient orchestration, horizontal scaling to adjust system capacity according to demand, while spreading the load across different nodes, and providing increased resilience. By combining the use of Docker, PySpark, blockchain, pBFT to establish a distributed consensus between the different nodes, artificial intelligence and Big Data, our approach benefits from enhanced decentralization, offering balanced task distribution, fault tolerance and better use of available resources.
[38]	- An incentive and security mechanism	- Enhanced security: Using real-time Big Data analytics and AI, threats are detected quickly. Blockchain enables robust authentication and transparent transaction traceability. In addition, compared with this reference's approach, which does not incorporate a consensus protocol, the decentralization and fault resilience offered by pBFT guarantee secure storage of sensitive data in smart city applications, and ensure continuous availability and rapid response to incidents. By using reliable data and making decisions based on it, we reduced the risk of cyber-attacks.
[39]	- Data sharing in mutual trust	- Data Sharing with increased trust: Unlike reference [38], in our approach we use Big Data with Hadoop and PySpark, which helps to strengthen data sharing and analysis with complete confidence. Thanks to their high processing capacity, these technologies enable large amounts of data to be managed efficiently in real time. In addition, by improving the quality of the data, reliable information is ensured, thereby boosting user confidence. Similarly, the use of pBFT in our approach provides a distributed consensus between different nodes to identify and reject malicious or corrupt nodes, and to agree on the verification or rejection of transactions or data modification. The protocol is more resistant to errors and manipulation of shared data, which improves trust, and the rapid agreement mechanism between nodes making data sharing faster and more efficient.
[40]	- Automated maintenance services and supply chain management	- Enhanced automated maintenance services and supply chain management: In our approach, the use of Docker improves automated maintenance services and supply chain management by offering environment isolation and rapid, reproducible deployment. Similarly, the integration of Big Data improves automated maintenance services by enabling predictive maintenance, while in supply chain management, it enables more precise planning, better inventory management and process optimization thanks to advanced analytics. In addition, the use of pBFT ensures the continuity of maintenance services and supply chain management by facilitating reliable operations, even in the presence of malicious nodes. This significantly reduces the probability of potential breakdowns and failures
[41]	- Privacy	- Enhanced privacy: In our approach, Docker offers environment isolation, while the use of pBFT guarantees data authenticity and integrity, mitigating the risk of falsification and illegal exposure of confidential data. The integration of secure Machine Learning algorithms and Big Data enables sensitive data to be examined, segmented and anonymized without compromising confidentiality, while simultaneously detecting potential threats.

From the analysis conducted in (Table 5), it is evident that our approach stands out from other main approaches for smart city cybersecurity due to its comprehensive nature and effectiveness through the use of blockchain technology that ensures security and immutability of data storage, pBFT protocol that ensures consensus between nodes even in the presence of malicious or faulty nodes allowing for increased resilience to potential attacks, and provides a higher level of reliability for all transactions. In addition, the use of artificial intelligence algorithms to detect anomalies and threats, as well as big data that provides valuable information that can be used to detect vulnerabilities, analyze trends and prevent security incidents. As a result, we can infer that our approach provides improved security, increased resiliency and better overall risk management for smart cities.

V. CONCLUSION

In this paper, we present a comprehensive and efficient approach for strengthening smart cities cybersecurity. Using blockchain, big data and artificial intelligence algorithms, this approach offers a robust and a reliable framework for smart cities data security and privacy. This framework was illustrated using a real dataset on smart grid, demonstrating its efficiency and reliability. By focusing on data confidentiality, integrity and availability, our approach allows to guarantee a secure environment for smart cities, their infrastructures and services while improving their resilience to cyber-attacks. In addition, this approach fosters mutual trust among the smart cities stakeholders and strengthens citizens confidence and engagement in smart cities applications and services.

FUNDING

This research received no external funding.

DATA AVAILABILITY STATEMENT

The authors confirm that the data supporting the results of this study are available within the article.

ACKNOWLEDGMENT

The author Abla El Bekkali would like to thank his father who supported him, his family, and his supervisors.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] A. Sharma, E. Podoplelova, G. Shapovalov, A. Tselykh, and A. Tselykh, ‘‘Sustainable smart cities: Convergence of artificial intelligence and blockchain,’’ *Sustainability*, vol. 13, no. 23, p. 13076, Nov. 2021, doi: 10.3390/su132313076.

[2] O. S. Neffati, S. Sengan, K. D. Thangavelu, S. D. Kumar, R. Setiawan, M. Elangovan, D. Mani, and P. Velayutham, ‘‘Migrating from traditional grid to smart grid in smart cities promoted in developing country,’’ *Sustain. Energy Technol. Assessments*, vol. 45, Jun. 2021, Art. no. 101125, doi: 10.1016/j.seta.2021.101125.

[3] F. Cui, ‘‘Deployment and integration of smart sensors with IoT devices detecting fire disasters in huge forest environment,’’ *Comput. Commun.*, vol. 150, pp. 818–827, Jan. 2020.

[4] T. Alam, ‘‘Blockchain-based big data analytics approach for smart cities,’’ Tech. Rep., Nov. 2020, doi: 10.36227/techrxiv.13054244.v2.

[5] T. Alam, ‘‘IoT-fog: A communication framework using blockchain in the Internet of Things,’’ *Int. J. Recent Technol. Eng.*, vol. 7, no. 6, pp. 1–10, 2019.

[6] R. Di Pietro, X. Salleras, M. Signorini, and E. Waisbard, ‘‘A blockchain-based trust system for the Internet of Things,’’ in *Proc. 23rd ACM Symp. Access Control Models Technol.*, Jun. 2018, pp. 77–83.

[7] D. Minoli and B. Occhiogrosso, ‘‘Blockchain mechanisms for IoT security,’’ *Internet Things*, vol. 1, pp. 1–13, Sep. 2018.

[8] K. Christidis and M. Devetsikiotis, ‘‘Blockchains and smart contracts for the Internet of Things,’’ *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[9] T. Alam, ‘‘Blockchain and its role in the Internet of Things (IoT),’’ *Int. J. Sci. Res. Comput. Sci., Eng. Inf. Technol.*, vol. 5, no. 1, pp. 151–157, Jan. 2019, doi: 10.32628/CSEIT195137.

[10] K. Abbas, L. A. Tawalbeh, A. Rafiq, A. Muthanna, I. A. Elgendy, and A. A. Abd El-Latif, ‘‘Convergence of blockchain and IoT for secure transportation systems in smart cities,’’ *Secur. Commun. Netw.*, vol. 2021, pp. 1–13, Apr. 2021.

[11] S. K. Singh, S. Rathore, and J. H. Park, ‘‘BlockIoTintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence,’’ *Future Gener. Comput. Syst.*, vol. 110, pp. 721–743, Sep. 2020.

[12] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir, ‘‘The security of big data in fog-enabled IoT applications including blockchain: A survey,’’ *Sensors*, vol. 19, no. 8, p. 1788, Apr. 2019.

[13] D. Bruneo, S. Distefano, F. Longo, G. Merlino, A. Puliafito, V. D’Amico, M. Sapienza, and G. Torrisi, ‘‘Stack4Things as a fog computing platform for smart city applications,’’ in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, San Francisco, CA, USA, Apr. 2016, pp. 848–853, doi: 10.1109/INFCOMW.2016.7562195.

[14] N. Deepa, ‘‘A survey on blockchain for big data: Approaches, opportunities, and future directions,’’ *Future Gener. Comput. Syst.*, vol. 131, p. 209 226, juin 2022, doi: 10.1016/j.future.2022.01.017.

[15] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, ‘‘Blockchain technology: A survey on applications and security privacy challenges,’’ *Internet Things*, vol. 8, Dec. 2019, Art. no. 100107, doi: 10.1016/j.iot.2019.100107.

[16] S. Abdullah, S. Rothenberg, E. Siegel, and W. Kim, ‘‘School of block–review of blockchain for the radiologists,’’ *Academic Radiol.*, vol. 27, no. 1, pp. 47–57, Jan. 2020, doi: 10.1016/j.acra.2019.06.025.

[17] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, ‘‘Everything you wanted to know about the blockchain: Its promise, components, processes, and problems,’’ *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6–14, Jul. 2018, doi: 10.1109/MCE.2018.2816299.

[18] Q. Wang, H. Zhao, Q. Wang, H. Cao, G. S. Aujla, and H. Zhu, ‘‘Enabling secure wireless multimedia resource pricing using consortium blockchains,’’ *Future Gener. Comput. Syst.*, vol. 110, pp. 696–707, Sep. 2020, doi: 10.1016/j.future.2019.09.026.

[19] X. Huang, Y. Zhang, D. Li, and L. Han, ‘‘An optimal scheduling algorithm for hybrid EV charging scenario using consortium blockchains,’’ *Future Gener. Comput. Syst.*, vol. 91, pp. 555–562, Feb. 2019, doi: 10.1016/j.future.2018.09.046.

[20] C. Yang, X. Chen, and Y. Xiang, ‘‘Blockchain-based publicly verifiable data deletion scheme for cloud storage,’’ *J. Netw. Comput. Appl.*, vol. 103, pp. 185–193, Feb. 2018, doi: 10.1016/j.jnca.2017.11.011.

[21] H. Chen and Y. Wang, ‘‘SSChain: A full sharding protocol for public blockchain without data migration overhead,’’ *Pervas. Mobile Comput.*, vol. 59, Oct. 2019, Art. no. 101055, doi: 10.1016/j.pmcj.2019.101055.

[22] A. K. Tripathi, K. Akul Krishnan, and A. C. Pandey, ‘‘A novel blockchain and Internet of Things-based food traceability system for smart cities,’’ *Wireless Pers. Commun.*, vol. 129, no. 3, pp. 2157–2180, Apr. 2023, doi: 10.1007/s11277-023-10230-9.

[23] J. Wu and N. Tran, ‘‘Application of blockchain technology in sustainable energy systems: An overview,’’ *Sustainability*, vol. 10, no. 9, p. 3067, Aug. 2018, doi: 10.3390/su10093067.

[24] N. Alasbali, ‘‘Rules of smart IoT networks within smart cities towards blockchain standardization,’’ *Mobile Inf. Syst.*, vol. 2022, Feb. 2022, Art. no. 9109300, doi: 10.1155/2022/9109300.

[25] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, ‘‘A survey on consensus mechanisms and mining strategy management in blockchain networks,’’ *IEEE Access*, vol. 7, pp. 22328–22370, 2019, doi: 10.1109/ACCESS.2019.2896108.

[26] R. Memon, J. Li, and J. Ahmed, ‘‘Simulation model for blockchain systems using queuing theory,’’ *Electronics*, vol. 8, no. 2, p. 234, Feb. 2019, doi: 10.3390/electronics8020234.

[27] A. Kiayias, A. Russell, B. David, and R. Oliynykov, ‘‘Ouroboros: A provably secure proof-of-stake blockchain protocol,’’ in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science). 2017, pp. 357–388, doi: 10.1007/978-3-319-63688-7_12.

[28] J. W. Roepert, ‘‘Digital supply chain—Die digitalisierung der supply chain mit Hilfe von IoT, machine learning, blockchain, predictive analytics und big data,’’ in *Logistik—Die Unterschätzte Zukunftsindustrie*. Wiesbaden, Germany: Springer, 2020, pp. 83–98.

[29] K. Rabah, ‘‘Convergence of AI, IoT, big data and blockchain: A review,’’ *Lake Inst. J.*, vol. 1, no. 1, pp. 1–18, 2018.

[30] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, ‘‘On security analysis of proof-of-elapsedtime (PoET),’’ in *Proc. Int. Symp. Stabilization, Safety, Secur. Distrib. Syst.*, in Lecture Notes in Computer Science, 2017, pp. 282–297, doi: 10.1007/978-3-319-69084-1_19.

[31] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, ‘‘Security services using blockchains: A state of the art survey,’’ *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 1st Quart., 2019, doi: 10.1109/comst.2018.2863956.

[32] S. Rakitin, A. A. Visheratin, and D. Nasonov, ‘‘Byzantine fault-tolerant and semantic-driven consensus protocol,’’ *Proc. Comput. Sci.*, vol. 136, pp. 25–34, 2018, doi: 10.1016/j.procs.2018.08.234.

[33] S. De Angelis, L. Aniello, R. Baldoni, and F. Lombardi, ‘‘PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain,’’ in *Proc. Italian Conf. Cyber Secur.*, 2018, p. 11.

[34] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, ‘‘Consortium blockchains: Overview, applications and challenges,’’ *Int. J. Adv. Telecommun.*, vol. 11, nos. 1–2, pp. 1–5, 2018.

[35] D. M. F. Mattos, F. Krief, and S. J. Rueda, *Blockchain and Artificial Intelligence for Network Security*. Cham, Switzerland: Springer, 2020.

[36] B. Bhushan, A. Khamparia, K. M. Sagayam, S. K. Sharma, M. A. Ahad, and N. C. Debnath, ‘‘Blockchain for smart cities: A review of architectures, integration trends and future research directions,’’ *Sustain. Cities Soc.*, vol. 61, Oct. 2020, Art. no. 102360, doi: 10.1016/j.scs.2020.102360.

[37] H. Yu, Z. Yang, and R. O. Sinnott, ‘‘Decentralized big data auditing for smart city environments leveraging blockchain technology,’’ *IEEE Access*, vol. 7, pp. 6288–6296, 2018.

[38] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18611–18621, 2019.

[39] G. Mujtaba and N. Javaid, "Blockchain based fleet management system for autonomous vehicles in an intelligent transport system," Tech. Rep., 2020.

[40] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain-based distributed framework for automotive industry in a smart city," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4197–4205, Jul. 2019.

[41] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7702–7712, Oct. 2019.

[42] *UCI Machine Learning Repository: Electrical Grid Stability Simulated Data Data Set*. Accessed: 2022. [Online]. Available: https://archive.ics.uci.edu/ml/datasets/Electrical+Grid+Stability+Simulated+Data+#

[43] D. T. Jose, J. Holme, A. Chakravorty, and C. Rong, "Integrating big data and blockchain to manage energy smart grids—TOTEM framework," *Blockchain, Res. Appl.*, vol. 3, no. 3, Sep. 2022, Art. no. 100081, doi: 10.1016/j.bcra.2022.100081.

[44] *Pearson Correlation Coefficient Formula*. Accessed: 2022. [Online]. Available: https://www.educba.com/pearson-correlation-coefficient-formula/

[45] M. Waseem, M. A. Khan, A. Goudarzi, S. Fahad, I. A. Sajjad, and P. Siano, "Incorporation of blockchain technology for different smart grid applications: Architecture, prospects, and challenges," *Energies*, vol. 16, no. 2, p. 820, Jan. 2023, doi: 10.3390/en16020820.

ABLA EL BEKKALI is currently pursuing the Ph.D. degree in cyber security with the Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes (ENSIAS), Mohammed V University. She has taught computer science and computer security in several engineering schools and universities, including UIR, EMSI, and INPT. In addition, she has authored numerous articles in the field of Internet of Things security.

MOHAMED ESSAAIDI (Senior Member, IEEE) is the General Manager of the Moroccan School of Engineering Sciences (EMSI) Group, General Manager (Since January 2023), Chief of Party of Interactive Digital Center Morocco (Morocco's XR training and innovation center, since November 2020) and a Professor and Past Dean of ENSIAS School of Computer Science of Mohammed V University, Rabat, Morocco (2011–2019), Past Director of International Cooperation at the Ministry of General Affairs & amp; Governance, Morocco (2019), and past faculty member Science of Abdelmalek Essaadi University, Tetuan, Morocco (1993–2011). He is the founder and past Chairperson of the IEEE Morocco Section (2005–2016), co-founder and chair of several IEEE OU in Morocco during the last two decades, including, IEEE ComSoc / Computer Society Morocco Chapter / IEEE Education Society Morocco Chapter / IEEE AP-S/MTT-S Morocco Chapter. He is IEEE IoT Global Cities Alliance, MEA Chairperson (2021–2022), IEEE Humanitarian Technologies Programs Committee Chair and IEEE Special Interest Group on Humanitarian Activities (SIGHT), Global Chair (since January 2023), IEEE EAB Teaching Excellence Editorial Hub, Member (2021–2022), and IEEE Public Safety Technology, Education Chair (2022). He is also a member of IEEE SA P2784 Smart Cities Planning and Technology Guide WG. He has authored and coauthored ten books and more than 200 papers in international refereed journals and conferences, in addition he filed ten patents, in the field of Electrical and Computer engineering and its diverse applications. In addition, he is the founder and the General Chair / co-chair of several IEEE technically sponsored international conferences such as Information and Communication Technologies International Symposium (2005, 2007), NATO Advanced Research Workshop on Information Security Assurance (2005), International Conference of Multimedia Computing and Systems series (2009–2016). He also co-organized and co-chaired IEEE Smart Cities Summit in May 2020, the US National Academies 5th Arab American Science, Engineering and Medicine Frontiers Symposium in November 2017, Rabat, Morocco and US NSF sponsored workshop on Smart Cities in January 2016 in Rabat, Morocco. He has also served in the Organizing committees and TPC and presented keynote talks at many other international conferences worldwide.

MOHAMMED BOULMALF is currently a Professor and the Dean of the School of Computer Science and Digital Engineering, International University of Rabat, Morocco. He served on technical program committee for several international and national conferences. He is the author/coauthor of many articles in fields of wireless networking and communications, wireless sensor networks, mobile computing, RFID technologies, and network security. In addition, he has been a reviewer of several international journals and conferences.