# Background

برگرفته از مقاله:‌ **A Trust-Influenced Smart Grid: A Survey and a Proposal**

The Smart Grid is the transformation of the traditional grid which can be combined with cyber devices to automate monitoring and control as well as include a two-way communication between systems [1]. The Smart Grid’s performance, just like that of the traditional grid, is centred on factors such as distribution, transmission, and generation. The coupling of the traditional power grid’s physical components and the cyber infrastructure has made the creation and continuous improvement of the Smart Grid possible. The diverse nature of the Smart Grid introduces varying applications and the integration of components such as electric vehicles, renewable energy resources, and variants of distributed power generators. Smart Grid has also introduced and improved vendorindependent standards that devices must conform to, thus allowing the seamless operation and integration of these devices into the Smart Grid.

Unfortunately, the cyber infrastructure’s integration into the power grid increases the attack vector of the Smart Grid, thereby making the security of the Smart Grid of paramount importance. In response, research has been undertaken under varying topics such as encryption [2], generation and management of cryptographic keys [3], privacy [4], risk assessment [5], and trust. Trust within the Smart Grid is important for determining whether an action, transaction, or communication is malicious or not. In the case of the notorious Stuxnet [6], there is the possibility that trust could have been implemented in devices to ascertain the legitimacy of malicious commands before responses or actions are taken on those commands.

## NIST Priority Areas on Smart Grid

The inclusion of a cyber infrastructure introduced a deficiency of myriad standards, which made maintaining the efficiency of the Smart Grid extremely challenging. In light of that, NIST identified nine key priority areas to be focused on to tackle these challenges [7]. These areas are discussed in this section.

### Energy Storage

One major challenge in the power industry is the storage of energy. Because of the immense difficulties posed by such storage, supply and demand are carefully balanced. This challenge brings about the need to invest and investigate new technologies to store energy, which will improve the efficiency within the grid from supplier to consumer.

### Wide-Area Situational Awareness (WASA)

Monitoring various components within the Smart Grid is salient to ensure their optimization. This guarantees that processes of demand and supply, as well as utilization forecasts, are facilitated. Thus, novel technologies and strategies are required to create tools that monitor and display these components within the Smart Grid.

### Advanced Metering Infrastructure (AMI)

Power usage by consumers is a key parameter in observing demand within the Smart Grid. In the traditional grid, meters were manually read and recorded before being computed to know the actual utilization within a given period. The introduction of the Smart Grid assures the near-real-time monitoring of power usage with AMI. AMI creates a dual-channel network between the smart meters and business systems of utility providers. This enables the collection and distribution of meaningful data to customers and utility providers as well as competitive retail suppliers. Such information can be used to implement residential demand responses. Even though there are many different designs of AMI, it consists of communications software and hardware and their associated system and data management software.

### Distributed Energy Resources (DERs)

DERs are resources that generate and/or store electricity for a local distribution system or a facility within that system. As such, DERs connect to these systems. DERs include combined heat and power (CHP) generators, electric vehicles/plug-in electric vehicles (PEVs), battery storage systems, solar panels, microgrids, and battery storage systems [8,9]. Because these technologies are relatively new, they continuously evolve. One key concern is using these resources to ensure a resilient, safe, and uninterrupted power grid and safeguarding the efficient generation, utilization, and storage of power from these resources.

### Distribution Grid Management

Distribution grid management systems integrate customer operations, networked distribution systems, and transmission systems with actual physical components, such as transformers, feeders, circuit-breakers and relays, to enable real-time functionalities such as the monitoring of system performances and load utilization [7]. Thus, the automation of distribution systems is important to operations of the Smart Grid, especially where systems such as AMI and PEVs are deployed to provide benefits such as reductions in peak loads, providing field engineers with malfunctioning devices’ locations, and increased reliability.

### Network Communications

Communication within the Smart Grid is important to ensure real-time monitoring, operations, and maintenance within the Smart Grid. Therefore, various technologies such as fibre-optics, wireless, and cellular (currently trending is 5G) are required in strategic areas or locations to aid in Smart Grid operations. Different routing algorithms are also required to ensure fast communication for the time-sensitive operations of some devices within the Smart Grid. Access to public and private communication networks will be required with various restrictions in place. Furthermore, critically important is ensuring that there is no collision or loss of messages during their transmission. Power network interfaces are required for long-distance transmission, and cost-effective solutions are always required. The efficient translation of protocols is also required as well as global standards to ensure that vendors can comply, thereby making communication seamless.

### Demand Response and Consumer Energy Efficiency

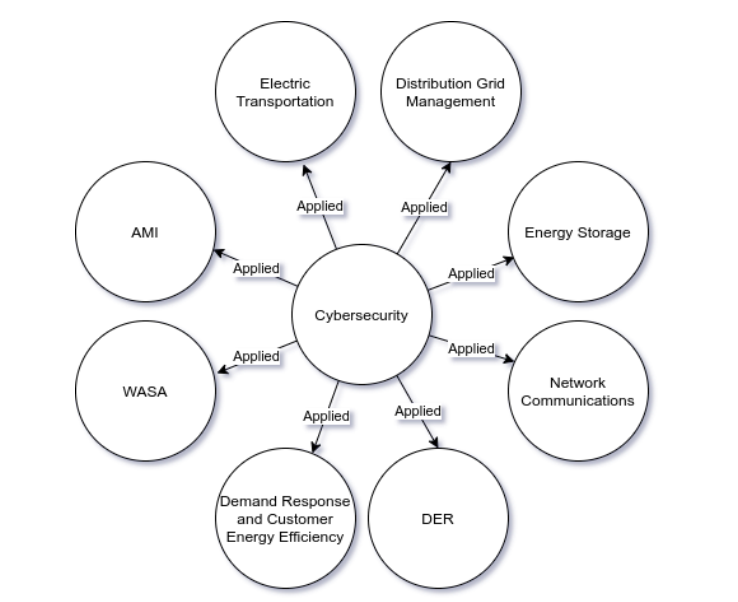
Technologies to balance supply and demand are being used by electricity suppliers and system planners. These technologies allow them to provide incentives (mostly financial) and mechanisms for consumers that lead to the efficient use of power during unstable power periods or peak periods. By providing detailed information to clients about consumption, they can save energy by engaging in practices and investing in devices that ensure the efficient utilization of power. Offering time-based rates such as critical peak rebates, variable peak pricing and time-of-use pricing can allow customers to take part in demand response efforts. Customers could allow utility companies to use direct load control programs to cycle water heaters and air conditioners on and off during peak periods in exchange for lower bill charges or incentives that may be financial or non-financial.

### Electric Transportation

Clean energy ensures reduced carbon emissions, reduced dependency on fossil fuel to drive the economy, and reduced carbon footprint for nations. Thus, the large-scale usage and patronage of PEVs are essential in ensuring that this happens. Technologies to ensure the cost-effective mass creation of these electric vehicles and their storage capacity are crucial to ensure that this happens.

### Cybersecurity

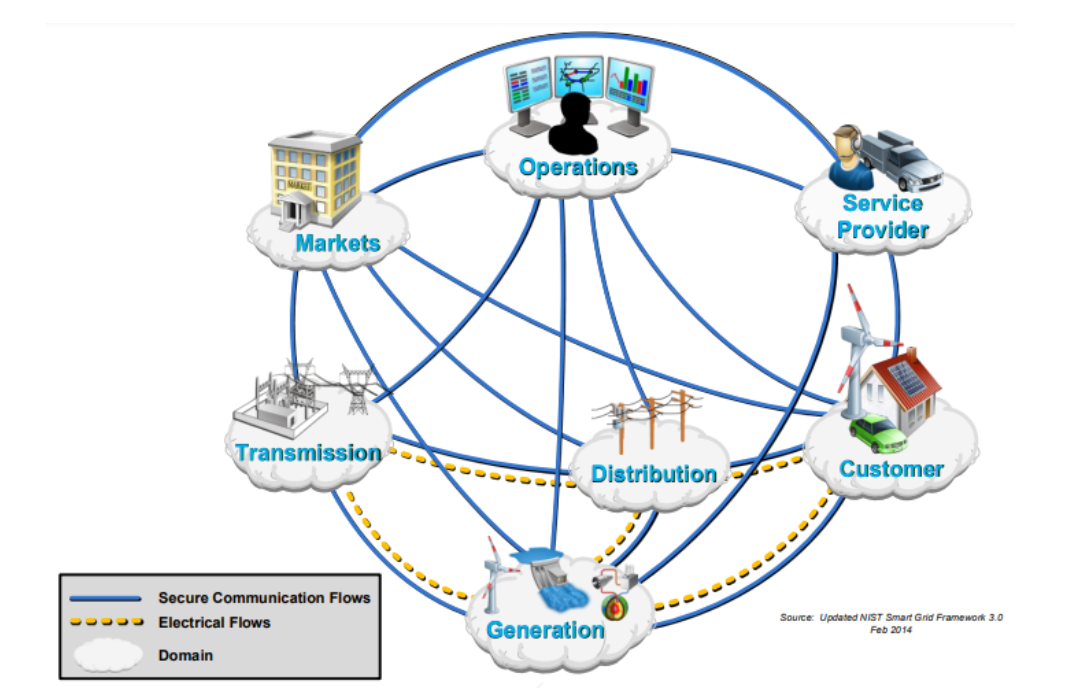
In a world where everything is being relocated to the cyber-domain, cybersecurity is critical to ensure the safety, availability, and reliability of the Smart Grid. It is very important to ensure that the operations of the Smart Grid are not adversely affected when security is applied within the grid. Cybersecurity plays a critical role in the operations of previously mentioned areas (Figure 1). There has been research into (but not limited to) network communication [10,11], demand response [12,13], PEVs [14,15], AMI [16,17] and DER [18,19]. This research includes encryption [19], privacy [20], intrusion detection and prevention [21], and trust. In this paper, we present a survey on the research on trust within the Smart Grid, especially within the priority areas and conceptual domains of the Grid. In terms of systems and trust, it is required that systems be cognitive to be able to trust each other. It is for this reason that we also investigate the application of trust in multi-agent systems’ research within the Smart Grid.



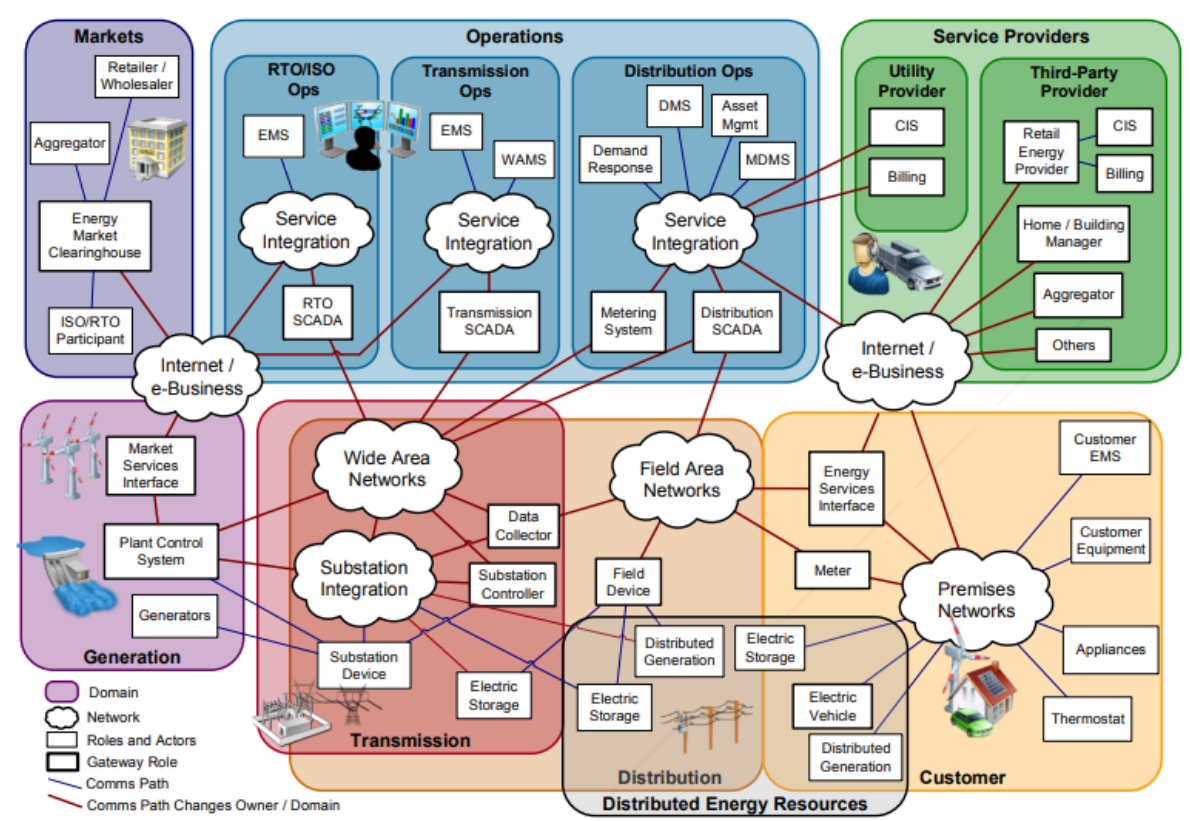
**Figure 1.** NIST priority areas: Importance of cybersecurity in priority areas.

## NIST Conceptual Domain Model

The conceptual domain model represents seven logical domains within the Smart Grid [7]. These domains represent the present and near-future view of the Smart Grid (Figure 2). The domains communicate with each other through interfaces. Figure 3 shows the mapping of legacy systems in the grid to the conceptual domains.



**Figure 2.** NIST conceptual domains [7].



**Figure 3.** Mapping of legacy systems to conceptual domain [7].

### Generation Domain

This is the domain where power or electricity is generated from renewable or nonrenewable forms of energy, and applications in this domain are the first processes when it comes to the delivery of power to customers [22]. It is from here that power is transferred to the transmission or the distribution domain. Thus, the connections with those two domains must remain reliable because power cannot be served to customers without it. Applications that can be found in this domain are asset management, protection, measurement, records/logging and control.

### Transmission Domain

The transmission domain is responsible for the bulk transfer of electrical power to the distribution domain from the generation domain through the use of multiple substations. A transmission network is usually managed and operated by a transmission-owning entity with the primary responsibility to ensure stability on the electrical grid by balancing supply (power generation) with demand (power consumption) across the transmission network. A Supervisory Control and Data Acquisition (SCADA) system, which comprises a communication network, control devices and field monitoring devices, is used to monitor the transmission network.

### Distribution Domain

The distribution domain is electrically connected between the transmission domain and the customer domain. The electrical distribution system may be structured in a varied number of ways such as meshed, looped or radial—and each structure affects the reliability of the system. Initially, the communications interfaces within this domain were unidirectional and hierarchical, but now they work in a bi-directional manner. Typical applications within this domain are measurement and control, substation, DERs, distribution generation and storage.

### Operations Domain

This domain ensures that the power system runs smoothly. A regulated utility is assigned the responsibility of ensuring this. Even though some of the functions in this domain may be provided by the service provider as the Smart Grid continuously evolves, there will always be core functions maintained in this domain. Typical applications in this domain are customer support, fault management, operation planning, monitoring, network calculations, maintenance and construction, analysis, records and assets, control, extension planning and reporting, and statistics.

### Service Provider Domain

The service provider domain provides support to other domains such as home energy generation, the management of energy use, and billing and customer account management. Its communication with the operations and markets domain is critical for situational awareness, system control and enabling economic growth. Typical applications in the service provider domain include building management, customer management, installation and management, account management, billing and building management.

### Markets Domain

The sale and purchase of grid assets are conducted in the Markets domain, hence its importance to ensure that communications within this domain are transparent and reliable. There is the balance of supply and demand as well as the exchange price within the power system that is ensured by this domain. It must also be noted that due to the evolving nature of the Smart Grid, the market domain is bound to evolve, which in turn will define the Smart Grid in the future. The market domain communicates with the entity that controls the assets (operations domain), the customer domain and the other domains that supply the assets. The efficient matching of demand for power with the consumption of power is dependent on the domain of the market; thus, the communication flow between that domain and the domains that supply the power is critical. Bulk generation and DERs (which are usually served through aggregators) are examples of power suppliers, with DER more likely to become greater partakers as the interactive nature of the grid increases. Typical applications in the market domain include market management, DER aggregation, market operations, trading, ancillary operations and retailing.

### Customer Domain

The customer is the main beneficiary of the Smart Grid and is the reason the Grid was created. The sole purpose of the customer is to consume the electricity generated by the grid. The customer domain is usually divided into home, commercial/building and industrial domains due to the difference in their energy demands. Each sub-domain has a meter and an interface that connects to other domains for utility-to-customer interactions. This may be done over the Internet or the AMI. Home or building automation is one of the applications in the customer domain that relies on these interfaces to function. Home automation allows the control of appliances within the house. Industrial automation, which is similar to home automation, also allows the control of industrial processes such as manufacturing. The interfaces also allow the storage of energy in thermal energy units and batteries as well as the generation of energy from renewable sources such as solar panels that are close to the customer. Although the customer domain communicates with and is electrically connected to the distribution and generation domains, it communicates with the service provider, operations, and market domains.

## blockchain

1. **برگرفته از مقاله:Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges**

Blockchain technology has gained much interest in recent years. Blockchain was first defined as a cryptocurrency [20] when it was first developed for digital money use. Blockchain was once thought to be Bitcoin, the most widely used cryptocurrency. However, blockchain is what really makes these digital currencies tick. It is a decentralized transaction ledger that several parties may use. Researchers initially had the least interest in this technology, but Bitcoin’s success ultimately swayed them. There was a sharp increase in the number of blockchain applications and usage in different technological areas after 2016. Financial services, medical care, manufacturing, and other sectors are among those which have implemented blockchain more deeply.

Blockchain is a chain of blocks of transactions recorded in series in which various administrators oversee the operation of classic client/server systems. Blockchain is a P2P network [21] in which all users have equal control over the network’s direction and operation. Many computers, or nodes, are linked together to form this network, and the blocks in the chain cannot be altered without the network’s consent. A record of the centralized database is stored locally on each node in the network [22]. The specifics of a given use case will determine the type of blockchain used. Public blockchains, private blockchains, and consortium blockchains are the three main categories of blockchain [23]. Three types of blockchains exist: public, private, and consortium. In a public or permissionless blockchain, no one may exert authority. Users are not restricted in their ability to read or write to the network. On the other side, private or permissioned ledgers are inaccessible to anybody who is not logged into the network as an authorized user.

The blocks are unreadable because they are protected with an encryption key. Consortium blockchains include both the public and private blockchain models. In contrast to centralized systems, the nodes in a blockchain network verify transactions among themselves in a decentralized manner [24]. Once a transaction has been verified by the nodes and uploaded to the blockchain, there is no way to undo it since the identification of the network nodes stays unanimous. So, the data stored on the blockchain cannot be altered [25].

While blockchain technology has shown promise for building a better infrastructure of the future Internet, there are still a number of issues that need to be resolved. Due to the immaturity of blockchain’s development, having access to knowledgeable individuals is essential. Businesses are understandably concerned about the hefty upfront infrastructure costs associated with BCT adoption, despite the many promising applications of this technology. Privacy and security considerations also play a role in the spread of blockchain technology. Legal considerations and difficulty scaling it up are also major concerns [26].

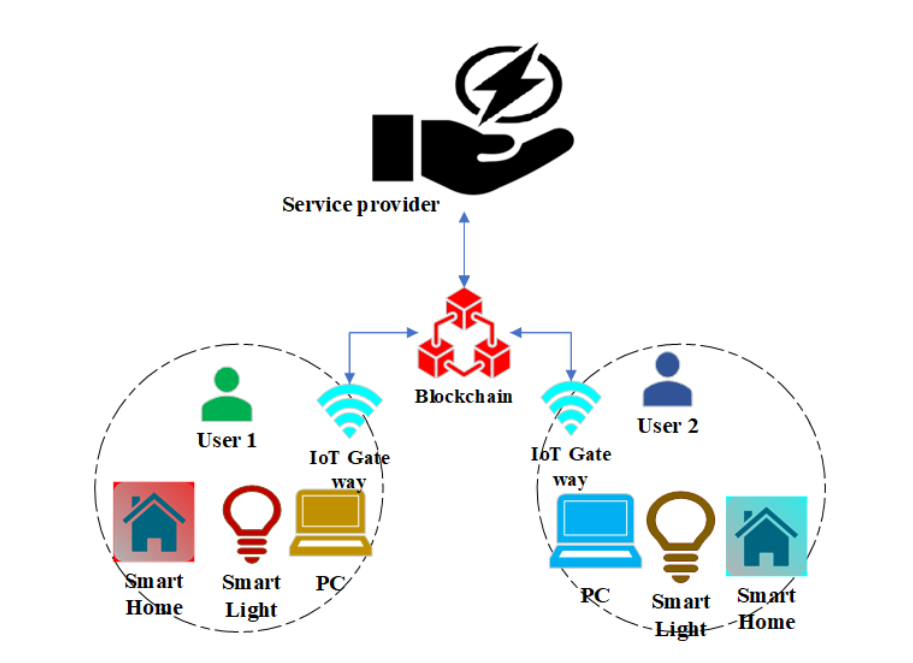
### Operation Blockchain for Smart Grids Applications

By fostering more trust and promoting greater decentralization, blockchain technology has the potential to alter existing applications drastically. However, the benefits it offers are not being fully used by SG applications despite its increasing expansion [30]

#### Blockchain for Home Automation

The resistance and RMS value of a current describe the conduction losses. The output is a smart home that is an IoT-integrated residence that improves the quality of life in many ways, including safety, healthcare, pleasure, and convenience. Technology for the home has improved the quality of life and allowed more people to live independently. Consumers and IT companies are interested in smart homes because of their valuable features, such as behavior tracking and safety assessments. Smart homes have many advantages for homeowners and others but are also susceptible to malicious cyberattacks that put consumers in danger [32]. Although there are existing methods for countering these threats, they are highly centralized and vulnerable to widespread assault. Because of this, the cutting-edge sector of automated smart home applications and facilities lacks the flexibility and scalability required for productive use. Several advanced technologies simplify people’s daily routines. These kinds of applications may produce massive amounts of data. There are security concerns associated with storing this dynamic content in archives. Blockchain has been shown to be a reliable and effective tool in the field of remote connection and data transfer in cybersecurity. As a result, it is being used for home automation [33].

Blockchain-based HA infrastructure refers to the use of several electronic gadgets (smart TVs, lighting, etc.), either working autonomously or in concert with one another to monitor the various settings of smart homes. To realize the potential of HA, these intelligent gadgets must be able to communicate with one another. An IoT gateway solves the problems that arise when several smart devices need to communicate with one another [34]. To prevent a security breach, such as to prevent users in one house from accessing the electronics devices in another house, the service provider is responsible for making control suggestions to the users’ smart devices on the basis of smart intelligent algorithms. Service providers may employ machine learning algorithms to provide more accurate suggestions and forecasts. Connecting consumers and service providers over a blockchain network improves HA security [35]. Possibly Ethereum or Hyperledger will be used to create the blockchain. A blockchain’s overarching design for HA is shown in Figure 3.

****

**Figure *3.*** Blockchain’s overarching design for HA*.*

Residents may only interact with the features of their own smart home devices and

cannot interact with the smart devices in the neighborhood’s smart homes. All household

gadgets may connect directly to the blockchain system through the gateway. Blocks containing device data may be linked using the blockchain’s hashing algorithm. The service

provider can provide data analysis and user-friendly recommendations, but it cannot

have access to a smart home’s actual gadgets themselves. Through the gateway, all of the

gadgets in a house may communicate with the blockchain network.

Challenges and Solutions: Many different blockchain technologies are being put to

use in HA-related projects right now [36]. Each system’s data are stored in a unique format, making integration difficult. Furthermore, these networks utilize various consensus

techniques. Interoperability across different blockchain platforms will only be possible if

they are standardized. A further difficulty in using blockchain for HA applications is performing real-time analytics on streaming data. They need to be analyzed and evaluated

in real time. For instance, real-time face detection is essential in an intrusion detection

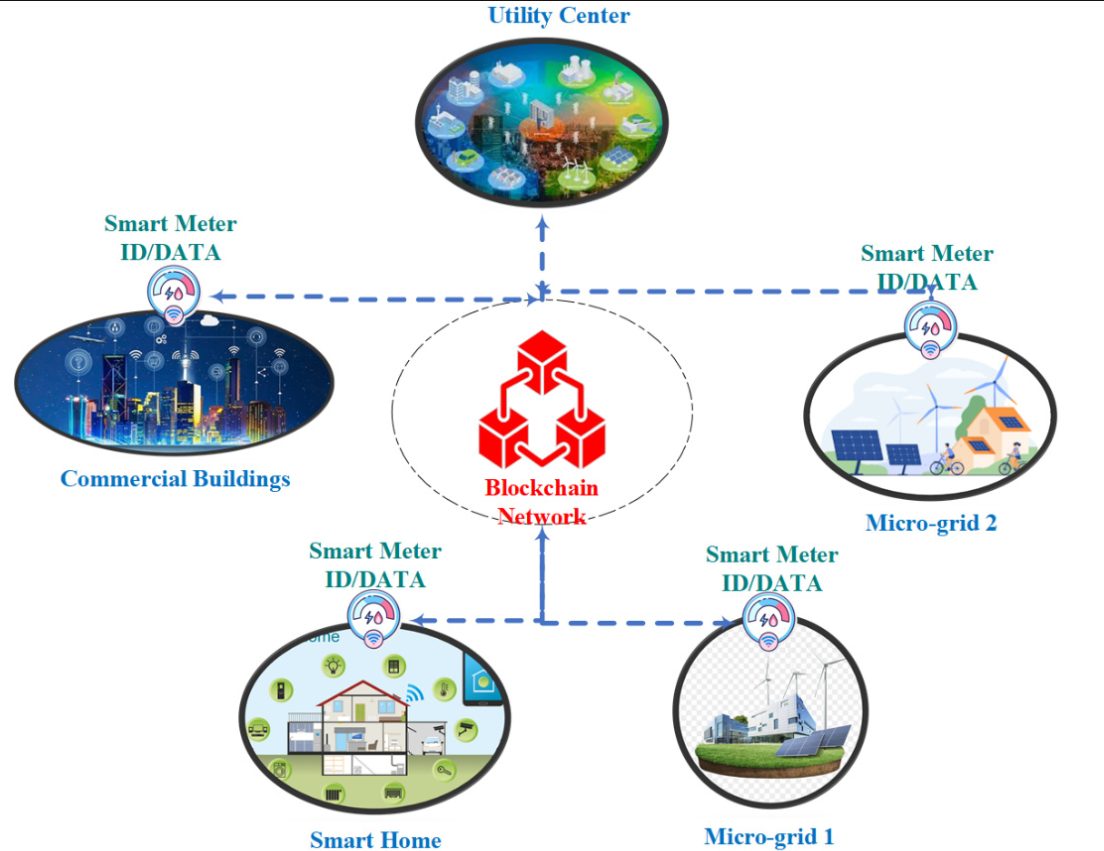
system. For real-time applications, processing blockchains might be difficult. Using a minimal framework might be the answer to this problem.

#### Blockchain for Advanced Metering Infrastructure

Every consumer’s energy usage data are collected, monitored, and sent through a smart meter; this meter is the brain of an AMI system. Many various groups have their own purposes for these meter data. The utility grid may use this information for demand forecasting and scheduling, while the distributor can utilize the information from smart meters to implement pricing structure and invoicing. On the other side, users may use this information for energy management purposes [37]. Despite the many benefits of AMI, transferring data across devices safely is difficult. A key component in reaching this goal is the blockchain-based AMI. Figure 4 presents a general approach for integrating blockchain technology into AMI. The gateway enables direct connection of the smart meters to the blockchain network [38]. In accordance with the IEC 62056 procedure, the meter readings will include meter identifiers and other data pertinent to the provision of utility services. The data from the AMI are sent to the meters, which are linked to the servers or nodes inside the blockchain network. All other nodes within the blockchain-enabled network are subsequently given access to these blocks. This network must be a private blockchain network accessible only by nodes affiliated with the utility hub. Without sacrificing privacy or

security, smart contracts and validations on a private blockchain may reveal inefficiencies in energy use. Challenges and Solutions: Despite the obvious benefits, blockchain technology has not been extensively used for this SG use case. Scientists have implemented it to improve the safety of AMI software. A lightweight blockchain-based infrastructure was presented in [39] for improving AMI security. This framework had a low energy footprint and was resistant to hacking attempts. Reference [40] demonstrates how blockchain may protect

AMI users’ private data. The same lack of interoperability and slowness in real time plagues the AMI blockchain, which also affects HA applications.

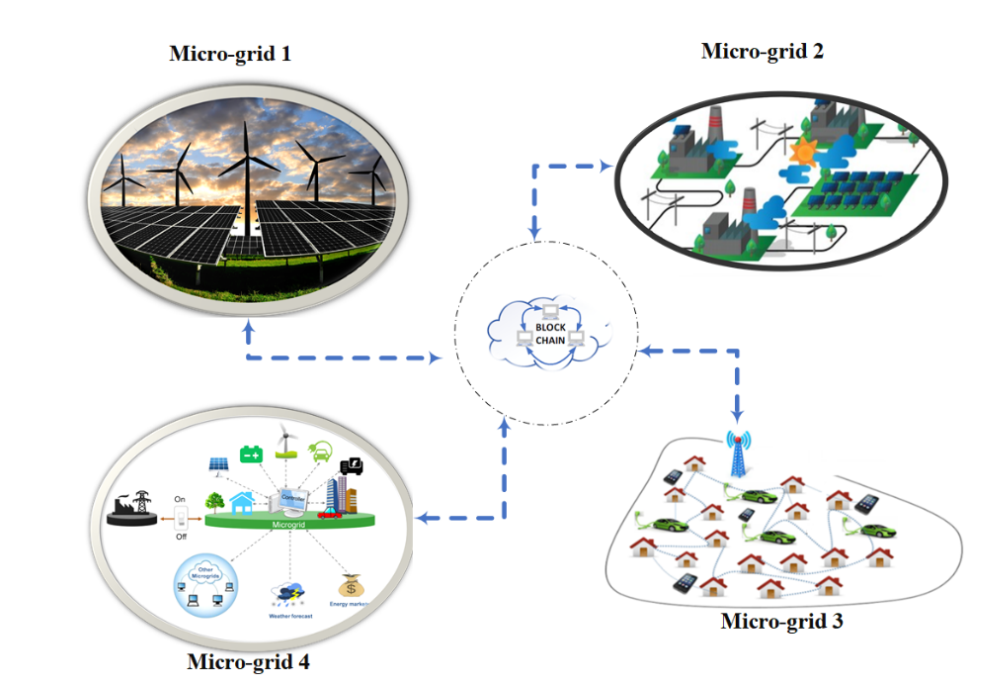


**Figure 4.** A general approach for integrating blockchain into AMI

#### Blockchain for Renewable Microgrids

Each day brings more evidence of the ongoing shift and development toward a

renewable grid based on a wide variety of decentralized energy sources, including solar panels, fuel cells, microturbines, batteries, and so on. Blockchain technology is essential to the smooth execution of these changes. Figure 6 depicts the MG application’s generic blockchain architecture. A zone’s electrical grid often covers a significant region, requiring many MGs to be considered. These many MGs are linked together through the blockchain system. Without compromising data quality or transparency, the blockchain network intends to improve safety and confidentiality in the MG operation. The produced energy, the power to be transferred with other microgrids, etc., are all included in the data block. Each freshly created block of MG data is verified by a consensus method to ensure its accuracy. After the block has been confirmed, it is added to the blockchain and the network. Blockchain nodes need appropriate algorithms to agree on the nature of the energy being transferred, the value of the power being sold, etc.



**Figure 6.** Blockchain architecture for MG.

Blockchain is viewed as a promising solution in renewable microgrids for efficient operation, such as complex point-to-point transactions between producers, traders, and users using intricate algorithms to validate, secure, and record these transactions. This is due to the growing community, financial, diplomatic, and environmental impacts and approaches, such as boosting power consumption, dealing with the middleman, market liberalization, and pollution. From a variety of angles, many authors have examined blockchain in the context of microgrids. The necessity of blockchain, its advantages, and its difficulties were discussed in [59]. Real-world solutions were provided in [11], including the Brooklyn Microgrid, which is based on a blockchain environment and uses the proof-of-work (PoW) mechanism. For individuals who want to suggest and execute workable solutions and approaches for renewable microgrids based on blockchain technology, additional thorough studies can be found in [60]. Furthermore, red. [61] presents an effective P2P blockchainbased energy market between a microgrid and a smart grid, with the distributed consensus algorithm being tested in the presence of a fault data injection attack (FDIA). In the face of cyberattack, this paper’s primary results demonstrated that the general agreement process continues, with the P2P market’s production response coming dangerously near to that of the centralized energy market. In keeping with the solution’s spirit, the authors in [62] proposed a concept for a blockchain-based incorporated energy management platform and a bilateral trading mechanism that, according to the simulation findings, significantly optimizes energy flow in a microgrid. In [60], a different model for blockchain-based energy systems was proposed, with a Pythagorean fuzzy technique proposed for selecting the optimal energy generation, distribution, and disposal. Results indicating greater profitability and lower CO2 emissions were also published in [63], which presents a different P2P energy trading method among the distributed generations based on the same technique employing a fuzzy meta-heuristic method as a pricing solution. In addition, the advantages of combining the power market with blockchain were investigated in [64] where transactions were emphasized utilizing a multi-agent coordination and trading model based on the Ethereum private blockchain. As we go further into the issue in this section, we find that blockchain applications vary depending on the underlying infrastructure technology of microgrids, such as in the case of AC, DC, or hybrid AC–DC MGs [65–67].

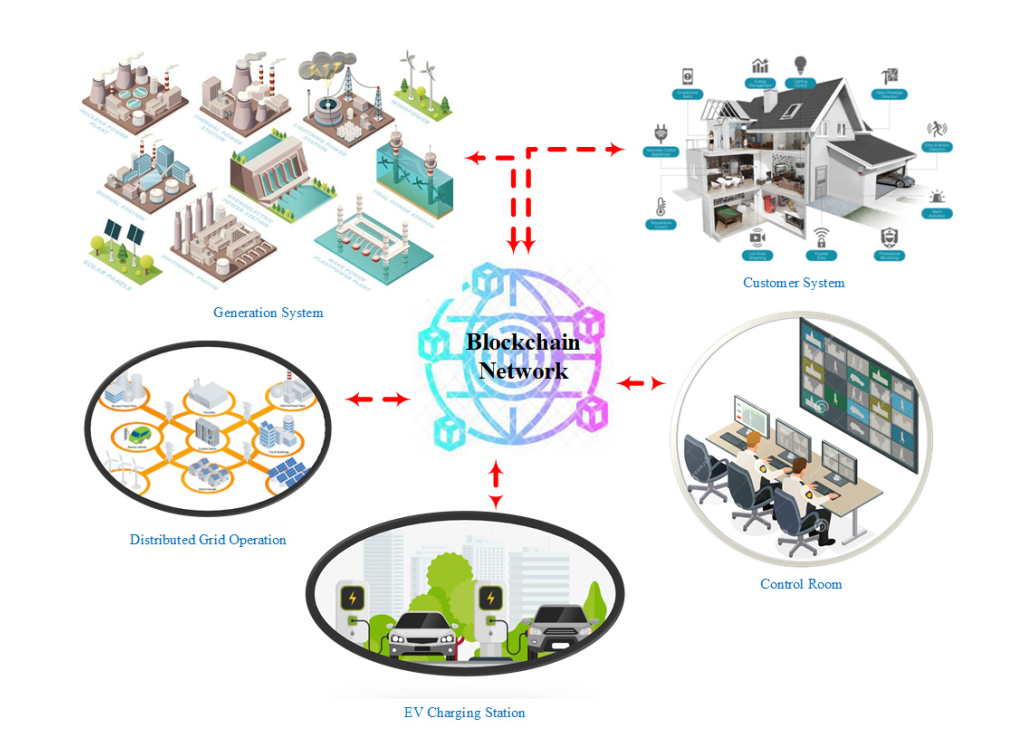
Challenges and Solutions: Blockchain-based renewable microgrids [68,69] provide many benefits but face significant obstacles. Limitations in technology, finances, society, the environment, politics and institutions, rules and regulations, social norms, and privacy and security from the beginning to the end are all obstacles to overcome. Key elements, such as privacy, resource management, restrictions, and prices, remain challenging to reconcile practically and effectively. Consortiums run microgrids in various ways; thus, evaluating and settling on the best algorithm or procedures to use; the most appropriate technology; the most appropriate investor; and a highly qualified workforce are essential

#### Blockchain for Energy Management System

A distributed system’s development and implementation by incorporating blockchain gives more advantages to both producers and users in the energy market. Wind and solar powers are becoming more popular sources of renewable energy, and as a result, the structure of the energy market and the need for safe energy transactions have evolved to accommodate this growth [70]. This can be accomplished with the use of blockchain technology. Energy marketing transactions have tremendous promise for blockchain’s distributed ledger technology. An EMS aims to facilitate trustworthy real-time trading of energy among all participants in the energy market, including but not limited to generating systems (including renewable and nonrenewable energy sources), consumer services, energy providers, etc. [62]. Figure 7 depicts the blockchain architecture used by an EMS.

The SG plans to combine alternative and traditional power plants. On the demand side, we have private residences, apartment complexes, office buildings, shopping centers, etc. Additionally, EV charging facilities are under the purview of SG shoppers. However, the entities in the consumer domain not only use power but also generate it. Prosumers are a term used to describe this kind of customer. Prosumers help ease the power grid’s strain when they store and use energy surpluses. While this relieves pressure on the power grid, it also makes it critical to track who buys and sells electricity. Safeguards to protect both parties’ personal information are equally crucial to the success of the energy marketplace. Blockchain technology may be included into the EMS to accomplish this goal. As depicted in Figure 7, the blockchain’s network seeks to connect all SG areas, including the generating system, the technical infrastructure, the consumption system, the regulator, and the control center. Through its distributed nature, interoperability, and smart contracts, the blockchain-based EMS protects the privacy and integrity of energy transactions. Private blockchains may integrate data controls and selective group access to guarantee safety and privacy in the energy trading market. The blockchain-based EMS improves transparency in P2P energy trading without jeopardizing users’ right to privacy because to its decentralized nature.

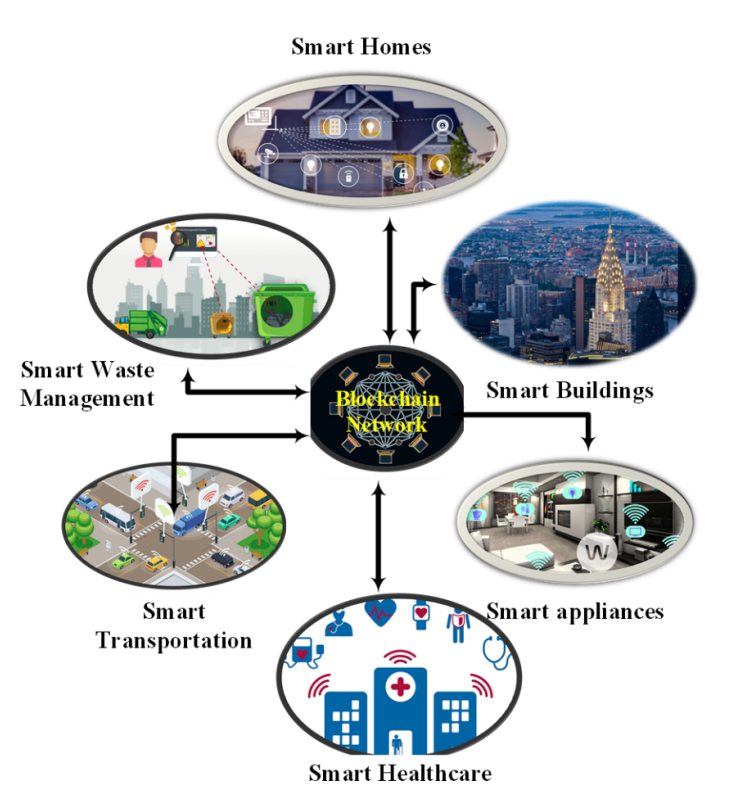
Challenges and Solutions: Challenges in trading arise as energy expenditures go up for which the trading system requires stringent regulation; it cannot be allowed to operate unchecked. Stringent management of this trading system is essential because as the energy trade rises, the challenges increase more. As a result, in [71], a mechanism for managing energy transactions online was presented, allowing customers to learn more about their own pricing and consumption habits. In ref. [72], Yi Zhang et al. addressed the security issue for users and energy flow. An online double auction-based energy market structure was presented by S.N.G. Gourisetti et al. in [73]. Because of blockchain technology, we can now have smart meters with extra privacy and safety features. Furthermore, a platform to monitor the energy produced from renewable sources by storing and selling energy between residences and communication networks of users was suggested in [74].



**Figure 7.** Blockchain architecture used by an EMS

#### Blockchain Smart City

The smart city framework is rapidly changing because of the proliferation of technologies such as blockchain, the IoT, and cloud computing. The future of the Internet of Things (IoT) will determine the design of “smart cities”, including the number and type of sensors and “smart objects” used to gather information about public facilities and services, as well as the availability of that information to the general public, the effectiveness of environmental safeguards, and the level of economic growth. Figure 8 depicts an overarching blockchain architecture for SCs [76]. It would be impractical to run all of the smart city’s services on the same blockchain network. Because of this, cities of varying sizes and types of smart services will need different configurations of blockchain networks. It is possible that each blockchain may be tailored to the specific needs of a particular application. Data generated by smart equipment (such as smart cars, smart houses, and smart hospitals) are recorded in a blockchain. To guarantee the services run well, we will need appropriate techniques and blockchain frameworks [77].



**Figure 8.** Overview of a blockchain architecture for SCs.

Some of the issues with smart city transportation were discussed in [78,79]. These studies showed how to use blockchain, which allows for the use of distributed stored data and performs transactions between producers and beneficiaries without the need for intermediaries, such as banks or governments, to improve public transportation and logistics [80,81], water supply [82,83], green energy [84,85], the environment [86,87], health [88,89], and education [90,91]. Smart contracts are becoming increasingly important in the evolution of transactions between parties, and blockchain architecture will bolster this trend. These contracts are initiated by either party’s actions (understandings) or by the readings of sensors, actuators, or Internet-of-Thing tags [92]. As a result, logistics, energy, the ecosystem, water management, health, and other sectors will all benefit from blockchain technology as they help transform communities into smart cities.

The study about applications of blockchain technology in different SG domains is summarized in Table 2 as follows [75].

**Table 2.** Applications of blockchain technology in different SG domains

**غیر از مورد Electric vehicles، بقیه موارد جدول دو می‌تواند آورده شود.**

### Blockchain-Enabled Cybersecurity System for Smart Grids

برگرفته از مقاله: A Trust-Influenced Smart Grid: A Survey and a Proposal

A compromised Smart Grid, or its components, can have cascading effects that can affect lives. This has led to numerous cybersecurity-centric studies focusing on the Smart Grid in research areas such as encryption, intrusion detection and prevention, privacy and trust. Even though trust is an essential component of cybersecurity research; it has not received considerable attention compared to the other areas within the context of Smart Grid.

برگرفته از مقاله:Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges

### Common Security Risks in Smart Grids

Smart grids provide a number of possible concerns that might affect both businesses and normal consumers. Customers’ personal information, among other sensitive pieces of data, may be at danger if the organization suffers any attack. Customers are vulnerable even when they are not online because enemies may attempt to snoop on them and steal private information. The percentage of cyberattacks is higher in the USA compared to any other country, which is 73%, while all other countries have cyberattacks less than 5%, and sector wise, the energy sector has the topmost level of cyberattacks, which is 51%. It is common knowledge that cyberattacks may severely damage the smart grid. Cyberattacks may compromise a smart grid’s availability, integrity, and privacy. Most cyberattacks may be broken down into a wide variety of subtypes, making it hard to list them all. The CIA Classification for smart grid attacks is listed in Table 3. This section will introduce several common forms of cyberattacks on the smart grid.

**Table 3.** CIA classification for smart grid attacks. **همه ش آورده بشه**

* + Denial-of Service (DoS) Attacks

Distributed denial-of-service (DoS) attack is a kind of cyberattack in which hackers send out false instructions to a server or network, causing the service to be interrupted, either momentarily or permanently, for the target audience [93]. To overburden systems and prevent incomplete queries, attackers repeatedly send many requests to the targeted computer or resource [94]. The standard DoS attack employs a single computer and a single communication link to overwhelm the target network or resource. Distributed denial-ofservice (DDoS) attacks are similar in nature but use a group of computers and networks to overwhelm their intended victim. Since it is hard to halt the attack by limiting a single source, the consequences of this attack might be far more severe [95].

Current denial-of-service and distributed denial-of-service (DDoS) attacks on smart rids target a variety of communication levels, including the application layer, the network and transport layers, the media access control (MAC) layer, and the physical layer [96]. Due to their poor computing capabilities, application-layer-based DoS/DDoS attacks can compromise millions of ICT devices in a smart grid [97]. Extreme data volumes are the mainstay of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks on the network and transport layers, slowing transmission bandwidth in the communication channels and ultimately impairing access for legitimate users. The quality of end-to-end communications is at risk from this form of assault [98]. To gain access to the network by reducing the performance of those who use the same communication channel, a DoS/DDoS attack at the MAC layer might deliberately tamper with the MAC settings. It is common knowledge that three types of frames (data frames, control frames, and management frames) are used to convey information at the MAC layer. While data frames are usually encrypted, management and control frames are not protected in the same way. As a result, denial-of-service and distributed denial-of-service attacks may disrupt the control and management infrastructure. It is a common practice for an attacker to use signal jamming to conduct a denial-of-service or distributed denial-of-service attack at the physical layer; all they need is a bridge to the communication channels. According to previous reports, jammer assaults on a smart grid may cause anything from delayed delivery of time-critical signals to a total denial of service [99].

* + False Data Injection Attack (FDIA)

FDIA may have detrimental effects on a power system because it can disrupt the state estimation process, leading the system operator astray [100]. State estimate is often a vital part of any control center. It takes raw sensor readings from the SCADA system, filters them, and then manipulates each bus’s status. Many power system applications rely on state estimates’ outcomes [101,102]. False and malicious data information may be used to deliberately mislead energy management systems’ control and monitoring functionalities (EMSs). Furthermore, a malevolent assault might lead to disastrous outcomes. The primary research foci are the theoretical foundations, practical implications, and countermeasures of FDIAs. The goal of the theoretical work is to develop injection vectors that can evade detection by the command-and-control server in a variety of scenarios. On the application side, i.e., energy management systems (EMS) and market management systems, the effect of FDIAs on power system functioning is evaluated (MMS). The primary responsibility of the defender is to provide system operators with effective defense tactics [103]. A legal FDIA may affect the electricity market and energy distribution and disrupt power system operations. Recently, Xie et al. [104,105] investigated both the ex-ante and ex-post effects of FDIAs in the electrical market. One of the goals of an assault is to increase one’s gain. As a rule, they aim to buy virtual power cheaply at one node and then resell it to other nodes via an FDIA for profit.

* + Phishing

Since phishing is so simple to do, it might be the initial step in exposing companies and their consumers to danger. Hackers may get access to sensitive information about an electricity company if its clients do not properly dispose of their bills and payment receipts [106]. However, employees may also face threats from inside the company, such as phishing emails that appear legitimate but really include malware that steals personal information. Giving information to unreliable sources and understanding the ramifications of these threats may have a privacy and financial impact on smart grid consumers. Hence, it is a major issue for designing a defense against phishing assaults [107].

* + Eavesdropping

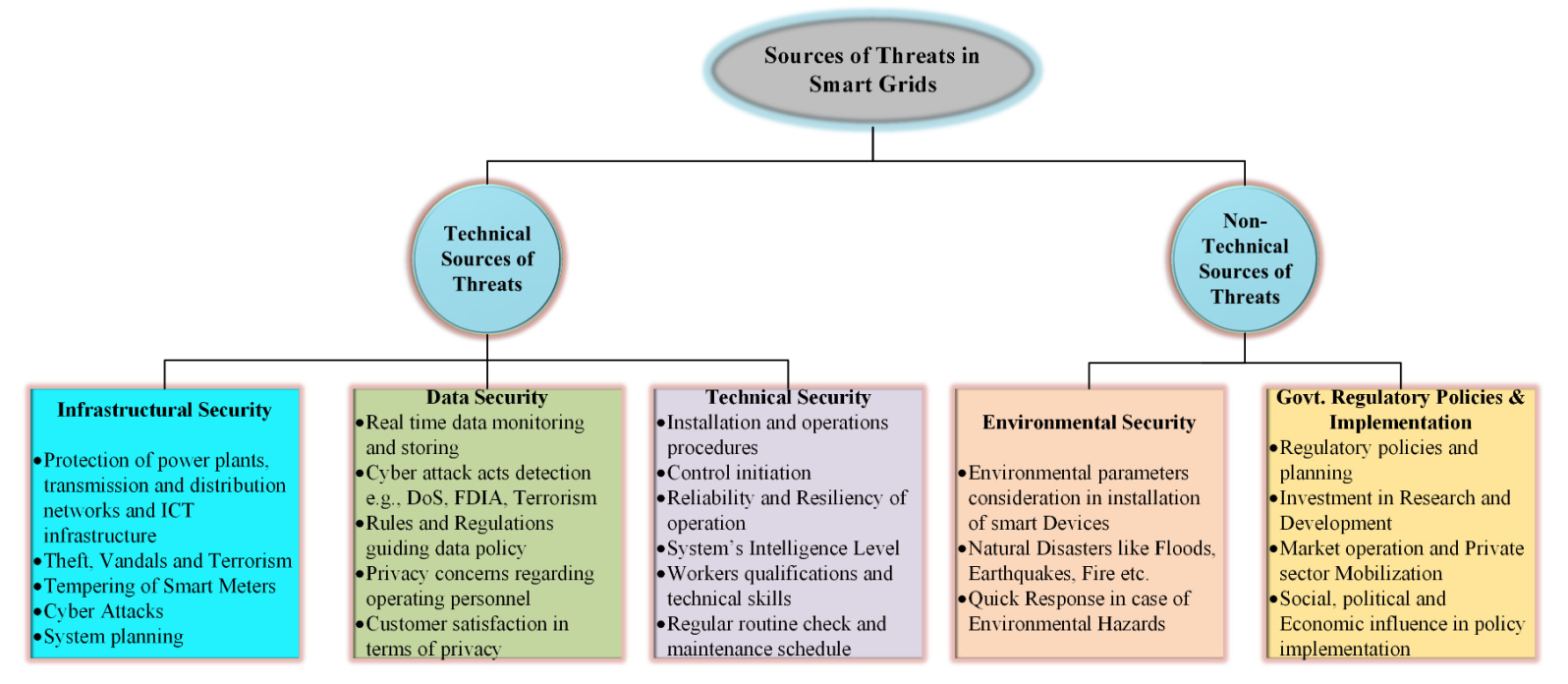
Some forms of spoofing attacks include eavesdropping and analyzing traffic patterns. The intruder may steal private data by eavesdropping on network traffic. Keeping the devices linked to the broader network, which a smart grid relies on, is challenging. Therefore, it poses a danger to the whole system. Most data security centers are concerned about smart grid since it presents the most significant threat of data theft [108].

* *Example of Security Breaches*
  + Stuxnet

Stuxnet is a dangerous computer worm that attacks SCADA systems (SCADA). In 2010, Stuxnet was discovered for the first time (Denning, 2012). It was speculated that the United States’ and Israeli spy services were responsible for developing the Stuxnet [111]. The harmful Stuxnet computer worm leverages the Microsoft Windows’ operating system and networks and is capable of manipulating programmable logic controllers (PLCs), which are responsible for managing the electromechanical operations of machines. The massive computer worm Stuxnet managed to enter the control system of Iran’s Nuclear Power Plant, where it manipulated the (PLCs) that regulated the centrifuges used to separate nuclear material, causing them to spin faster than normal and rip the machinery apart [112]. In response to the Stuxnet computer virus, the specialized machinery increased their rotational speed and promptly began damaging the nuclear fuel. While Stuxnet itself poses little threat to infected machines, it does perform a check to determine whether the infected machine is linked to certain Siemens PLC types. The United States and Israel designed Stuxnet to stop Iran’s nuclear weapon development.

* *Countermeasures against Cyberattacks*

Concerning cybersecurity in smart grids, the information and communication networks are particularly exposed to threats and hazards. Practicing certain security risks preferably requires a security solution to guard against vulnerabilities. The greatest challenge to a network and system is the dangers and threats that it faces. Figure 9 shows the classification of smart grid attacks and threats from different sources. Protecting the integrity of a smart grid system and its data requires a proper protection scheme that can counterattack to a wide range of cyberattacks. It is believed that using many defensive measures at different detecting nodes may achieve a protected and secure system. A distributed denial-of-service (DDoS) assault is one of the most significant dangers to a smart grid because it may cause the breakdown of the communication networks and control systems that are the foundation of the smart grid. The two types of strategies against DoS attacks followed by a discussion of additional counterattacks for smart grid is given as follows.

**Figure 9.** Classification of smart grid attacks and threats from different sources.

* + Encryption

The stated encryption encodes data so an unauthorized party cannot decode them. Any piece of information that is encrypted and then any data that the hackers intercept are useless in the form of raw code. Encryption may be seen as a kind of hidden coding. A cipher is the method by which your information is encrypted, and a key is the set of rules that enables you to read the message again [120]. The most highly rated VPN services use 256-bit AES (Advanced Encryption Standard), the industry’s strongest encryption standard, where 256 is the length of the encryption cipher being employed. With 256-bit encryption, the number of possible permutations exceeds the number of stars in the Milky Way. Banks and governments all across the globe rely on this degree of encryption to protect their sensitive information [121].

* + Authentication

Robust authentication systems are of utmost importance in situations when it is necessary to maintain authentication and manage access [122]. An “implicit deny policy” may be useful in implementing authentication and the policy’s usage in allowing only explicit users access to the network. This policy provides the business with security solutions and allows for the differentiation of rights across users (e.g., management can view all extra data linked to projects, while workers have restricted access to data). By limiting access to trusted employees, you can lessen the likelihood of a security breach and know exactly who logged in. In addition, SSL protocols may be used to perform authentication. Cyberattacks, such as denial of service, might compromise the protocols [123]. Because of the increased bandwidth needed for communication inside a smart grid network, cryptographic methods may be employed for authentication [124].

* + Network Security

VPNs allow users to increase their protection while connecting to a public network through the Internet. Using public network infrastructure puts sensitive information at risk, thus a virtual private network (VPN) employs a number of security measures, including encryption, to safeguard data in transit. Furthermore, virtual private networks (VPNs) are employed for communication since they provide a safe channel for data transfer. There are two distinct VPNs, both of which provide advantages to businesses and their frequent customers [126]. Remote access virtual private networks (VPNs) allow users to connect to internal company networks through a public network. After authenticating, users on mobile devices and desktop computers will be able to access the VPN server. When the credentials are right, the authentication is able to confirm access and provide access to the virtual network’s resources. An organization’s proprietary apps and data are among the resources that are accessible solely inside the company. Connecting to a VPN gateway allows users of the remote access VPN to perform their duties from any location. Virtual private networking (VPN) between two sites is quite similar to VPN access from a remote location. However, it often links the whole network in a single spot, even if the networks themselves are situated elsewhere; this is helpful for a bigger company that has to safely share its resources with several outposts in different areas to serve its partner or client business [127].

## Trust

برگرفته از مقاله:‌ **A Trust-Influenced Smart Grid: A Survey and a Proposal**

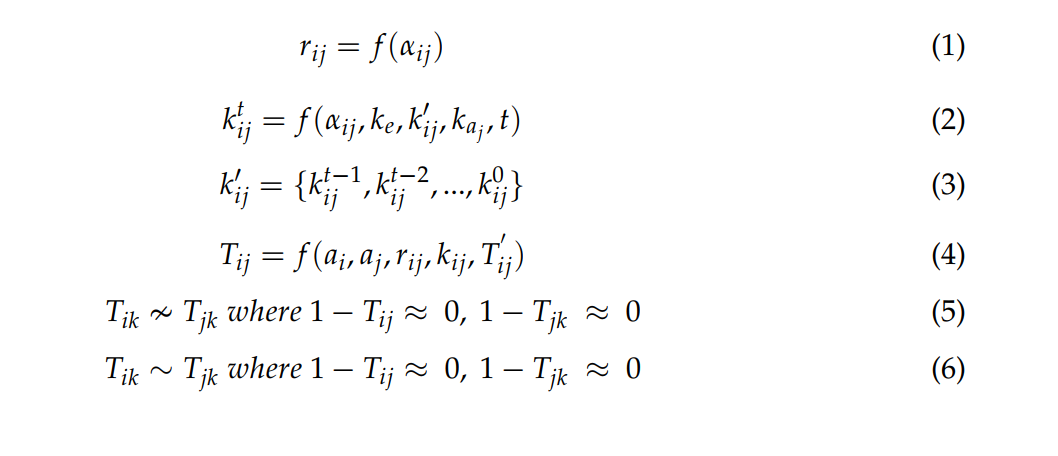
The world would not function without trust. Without trust, it would be difficult for interactions and/or transactions to exist. As a concept, trust is fundamental in the building and maintenance of stability in human relations. Trusting someone or something helps create interactions between people and organizations. In the digital age, with the current existence of virtual markets and communities, the interest in trust has matured and as such, can be expanded into other domains. Thus, any effort undertaken towards the proper management of trust by sharing information that enables interactions between participants in the open environment is essential and challenging. It is worth noting that trust is only useful in uncertain situations where people or agents must cooperate to achieve goals.

### Trust Definition and Formalization

According to the literature, trust has many definitions. A definition from the social sciences states that trust is the degree of subjective belief about the behaviours of a particular entity [23]. Trust is also defined as an agency’s subjective probability of performing a particular act [24]. In this paper, we define the trusting entity as the *agent* and the entity being trusted as the *subject*. Marsh [25] describes three levels of trust, namely basic trust, general trust, and situational trust. Basic trust is the general trusting disposition of an agent. General trust is the trust that an agent has on a subject at a certain time. Situational trust is the trust that the agent has on the subject, taking into account a certain situation.

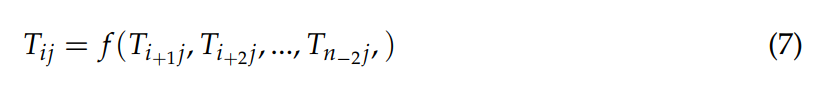
It must be noted that trust has been applied in different contexts, thus the notion that trust has many definitions. Thus, the design of trust models is required to be within a context or in terms of the system being designed. Thus, the factors being chosen to design the trust model must be on objective grounds to ensure that the trust being modelled is also objective. Hence, the difficulty in modelling trust. Regardless, trust models must have a component that must accept the risk because, without the assessment of risk, there is no trust.

NIST defines risk as: *A measure of the extent to which an entity is threatened by a potential circumstance or event* [26]. Thus, for an agent, *ai*, and a subject, *aj*, we define the risk, *rij*, of a transaction, *aij*, involving *ai* and *aj* as a function as shown in (1). There must also be a component of knowledge, *ktij*, within the trust model. Before and after a transaction, knowledge about *aij* and previous transactions (*k0ij*) with the subject, the environment (*ke*), knowledge of *aj*, *kaj*, and the time period (*t*), are also of prime importance in determining trust. We formulate knowledge as shown in (2). *k0ij* is a collection of transactions before the current transaction, and this is formulated in (3).



Thus, with risk, *r*, and knowledge, *ktij*, the decision on trust can be made. Therefore, trust, *Tij*, can be expressed as the output of a function that takes a tuple of elements as shown in (4) where *Tij 0* is the previous trust value between *ai* and *aj*. The *Tij 0* has an influence on the decision for *ai* to trust *aj* to undertake *aij*. Trust is represented as a continuous variable over a specified range usually *-*1 *≤ T ≤* 1 or 0 *≤ T ≤* 1 where 1 represents complete trust, *-*1 represents complete mistrust and 0 represents no trust. It must be noted that the transitive property of trust may or may not exist. In a situation where it does not exist, for three agents *ai*, *aj*, and *ak*, the fact that *ai* trusts *aj* and *aj* trusts *ak* does not mean that *ai* trusts *ak* (see (5)). In a situation where transitivity exists, it means that *ai* trusts *aj* and *aj* trusts *ak*, therefore, *ai* trusts *ak* (see (6)).

Trust can be directly or indirectly evaluated. Direct trust is calculated based on direct interactions between the agent and the subject. The default definition of trust is direct trust and that is formulated in (4). In the situation where no interaction exists between the agent, *ai*, and subject, *aj*, trust is built based on opinions from other agents about the subject; this is termed indirect trust. As formalized in (7), in an environment of *n* agents, trust is computed based on the recommendation of, at most, *n -* 2 agents.



### Trust-Based Attacks

In ensuring that trust mechanisms do not work in an environment, adversaries employ different attacks or strategies [27,28]. Some of these attacks are as follows:

•*Misleading feedback attack:* In this attack, a compromised agent feeds bad reports or

recommendations to other nodes to denigrate agents with good reputations. It is also

known as bad-mouthing attack or betrayal attack.

• *Sybil attack:* This attack involves a malicious agent within the system creating fake

identities to create a larger influence over other agents using false rankings.

• *Newcomer attack:* This attack involves the malicious agent reintroducing itself as a new

agent within the system in an attempt to erase its history of bad scores.

• *Ballot-stuffing attack:* In this attack, malicious agents collude by providing inaccurate

recommendations or reports in an attempt to take over the system. It is also known as

collusion attack.

• *On–off attack:* This attack involves a malicious agent repeatedly switching between

being honest and dishonest in an attempt to be undetected. It is also known as

inconsistency attack.