frontiers | Frontiers in Energy Research

ORIGINAL RESEARCH
published: 26 May 2022
doi: 10.3389/fenrg.2022.892066

Secure Transmission and Intelligent Analysis of Demand-Side Data in Smart Grids: A 5G NB-IoT Framework

*Yongpeng Shen[1], Ting He[1], Qian Wang[1], Junmin Zhang[2] and Yanfeng Wang[1]**

[1]College of Electrical and Information Engineering, Zhengzhou University of Light Industry, Zhengzhou, China, [2]Pinggao Group Intelligent Power Technology Co., Ltd., Pingdingshan, China

In order to tap the advantages of Narrow Band-Internet of Things (NB-IoT) on the demand side of the smart grid, improve the security of information transmission, and make use of demand-side data, we focus on the secure transmission, trusted services, and intelligent analysis of “5G + Smart Grid,” and we construct a comprehensive solution which consists of encrypted data terminals, management systems, and intelligent analysis methods. A 5G NB-IoT framework proposed in this study can serve grid planning and demand response, and it can further promote the deep integration of 5G and the smart grid. Therefore, this research will contribute to the implementation of a new generation of information technology on the smart grid, build a deep integration application scenario of the “5G + Smart Grid,” improve the intelligence of the grids, and further promote the “dual carbon” goal of the power system.

Keywords: NB-IoT, the smart grid, security transmission, demand-side data, information technology

OPEN ACCESS

Edited by:
Yongxi Zhang,
Changsha University of Science and Technology, China

Reviewed by:
Yu Wang,
Guangdong University of Technology, China
Yitao Liu,
Shenzhen University, China

****Correspondence:***
Yanfeng Wang
wangyanfeng@zzuli.edu.cn

Specialty section:
This article was submitted to Smart Grids,
a section of the journal
Frontiers in Energy Research

Received: *08 March 2022*
Accepted: *14 April 2022*
Published: *26 May 2022*

Citation:
Shen Y, He T, Wang Q, Zhang J and Wang Y (2022) Secure Transmission and Intelligent Analysis of Demand-Side Data in Smart Grids: A 5G NB-IoT Framework.
Front. Energy Res. 10:892066.
doi: 10.3389/fenrg.2022.892066

1 INTRODUCTION

The smart grid is an electricity network that can cost-efficiently integrate the behavior and actions of all users, including generators, consumers, and those that both generate and consume, in order to ensure the power system is economically efficient and sustainable with low losses and high levels of quality, security of supply, and safety (TEN-E, 2017). The smart grid uses the IoT technology to add intelligence and monitoring to every node. The applications of the smart grid can balance the flow of power more efficiently. They can detect surges, outages, and energy waste. They can also deal with peak loads or fluctuations immediately and automatically.

With large-scale access to renewable energy sources such as wind, solar, and electric vehicles, and distributed access to demand-side energy storage, the power system is changing dramatically. The power system is becoming more diverse in terms of forms of energy supply, massive amounts of data, and ways of interaction and control.

The demand side is the “nerve ending” of the smart grid, which has the characteristics of a large number of terminals and extensive connection of equipment. A safe, reliable, and intelligent demand side is the cornerstone of the power system. Two-way communication among generators, transmitters, and customers is the key to the smart grid. This mutual intelligent system offers solid benefits, including energy management, reliability and resilience, and the integration of intermittent renewable energy generation and storage. It also accommodates distributed power generation and microgrids, enhances the value of electric vehicles, and gives customers greater choices of how and when to use electricity (IIOT Power, 2019; Xu et al., 2020a; Xu et al., 2020b; Yuan et al., 2021).

The downside of the smart grid is how to interact with each other between those interconnections—driven by IoT technologies, data flow, and information management. In terms of its nature, do the disadvantages offer cybersecurity threats, opportunities for malevolent forces to intrude, disrupt, or destroy? (IIOT Power, 2019).

Most of the research studies on demand-side information security by scholars belong to the scope of a home area network (HAN) and a neighborhood area network (NAN) in the advanced metering infrastructure (AMI) framework, which can be divided into two categories: one does not use any encryption means, but other methods are used to ensure the security of demand-side information, such as connecting batteries and other equipment on the user side, or adding noise to the demand-side information artificially (Yuan et al., 2020; Tan et al., 2013; Lang et al., 2022; Chen et al., 2013). The aforementioned methods ensure the safety of the user's personal information but reduce the usability of the information. Lu et al (2012) proposed a privacy protection and data aggregation scheme based on homomorphic encryption, which can prevent the leakage of user privacy during smart grid communication. Abdallah and Shen (2015) proposed a lattice-based number theory research unit (NTRU) public key cryptosystem with low computing resource consumption, which enabled the use of a more secure public key cryptosystem in the demand-side network while still achieving low computing resource consumption. Nicanfar et al (2012) proposed an identity-based public key encryption system to construct an identity authentication strategy suitable for a HAN. Jokar et al (2011) proposed an intrusion detection scheme at the physical layer and 802.15.4 Media Access Control (MAC) layer to determine whether the HAN has been invaded by detecting signal strength, data size, format, and flow direction. Sanduleac and Ciornei (2021) proposed a general framework for extracting technical knowledge from high reporting rate smart meters (HRRSM) data to strengthen distribution system operator (DSO) monitoring tools to protect the privacy of users.

Through the analysis of the aforementioned secure transmission methods, the following conclusions can be drawn.

1) At present, the demand side mostly adopts the neighborhood area network and local area network framework in the AMI framework, and the advantages of the 5G Massive Machine-Type Communication Wide Area Network (mMTC WAN) have not yet emerged.
2) The current research studies only focus on the efficiency and structure of transmission but have not paid enough attention to the issue of information security transmission in the context of a two-way interaction.
3) How to use intelligent approaches to increase the value of demand-side data requires urgent attention.

In response to the aforementioned problems, we focus on the secure transmission, trusted services, and intelligent analysis of the "5G + Smart Grid" and construct an all-round solution consisting of encrypted data terminals, management systems, and intelligent analysis methods. The proposed "5G + Smart Grid" framework can service grid planning, demand response, and promote the deep integration of 5G and the smart grid.

The rest of this article is organized as follows. In **section 2**, the features of the demand side of the smart grid are analyzed. **Section 3** describes the overall technical framework of the proposed 5G NB-IoT secure transmission and intelligent analysis of demand-side data in the smart grid. **Sections 4–6** describe the secure transmission system, trusted service management system, and data intelligent analysis system in detail, respectively. Finally, the conclusion is stated in **section 7**.

2 ANALYSIS OF THE DEMAND SIDE IN THE SMART GRID

We consider the demand side in the smart grid that contains a distributing substation, distributed power source, distributed energy storage, industrial electricity supply, and residential electricity supply, as shown in **Figure 1**. Sometimes, the concepts of the distributed power source and distributed energy storage are confused. For example, electric vehicles are both distributed power sources and distributed energy storage. Photovoltaic power stations as distributed power sources may also be equipped with energy storage, to become distributed energy storage.

Generally, each distributed power source, distributed energy storage, industrial electricity customer, and residential electricity customer is connected to the distribution network through a smart meter (SM). In industrial application scenarios, various pieces of electrical equipment are connected to the mains through smart sockets (SS), such as lighting equipment, charging equipment, hoister, blowers, heaters, refrigerators, air conditioners, water heaters, cookers, and washing machines. The Intelligent Distribution Trans-former supervisory Terminal Unit (iTTU) is responsible for monitoring the working status of transformers and the entire distribution network.

In the next-generation power distribution network, each iTTU, SM, and SS is responsible for monitoring the voltage, current, active power, reactive power, and other information of relevant nodes. They must have communication functions to transfer the grid data to the data center in real time for further analysis. The basic features of the next-generation demand side in the smart grid can be summarized as follows.

1) Large number of nodes.

As mentioned previously, on the demand side of the smart grid, each node will have at least one SM. Each electrical apparatus will be connected to the mains through SS. It will result in a user having dozens of data nodes, while a power distribution network will have thousands of data nodes.

2) Many application scenarios.

The application scenarios on the user side include a distributing substation, distributed power source, distributed energy storage, industrial electricity supply, residential electricity supply, smart power distribution, and others. At the same time, it covers multiple stakeholders, such as equipment manufacturers, telecom operators, and users. Once a data leakage

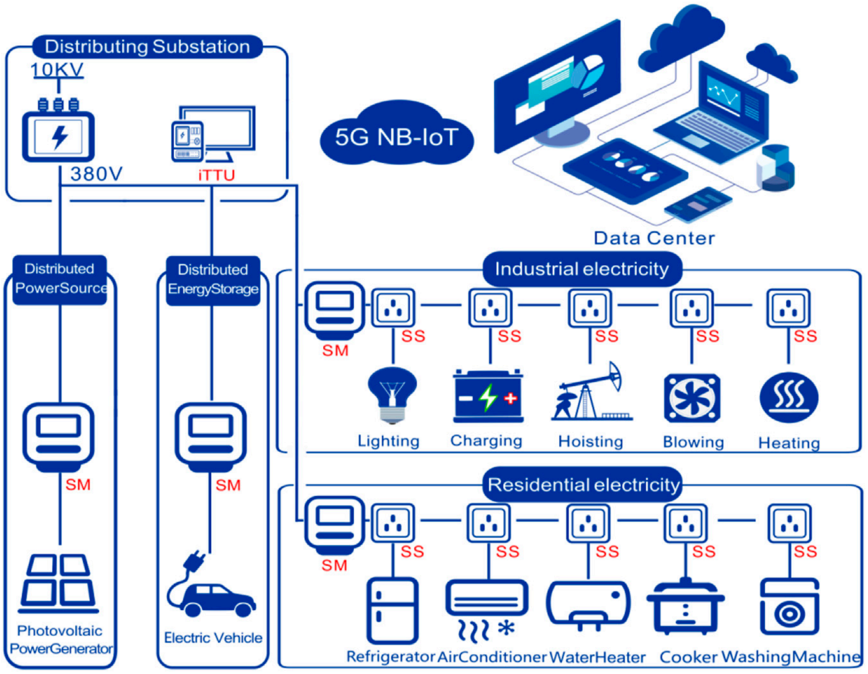


FIGURE 1 | Demand side in the smart grid.

problem occurs, it is difficult to clarify the security responsibilities.

3) Fast iteration speed and emerging security upgrade risks.

At present, the communication architecture of the smart grid has not yet been unified, the business and profit models have not yet been clarified, and the communication protocol between the various entities has not yet formed a unified standard; meanwhile, with the rapid development of the smart grid, new things and new models are constantly emerging. Therefore, smart grid data terminals must have high-security upgrade management functions and convenient software iteration speed to adapt to the new models and new requirements.

In view of the aforementioned characteristics of the demand side of the smart grid, combined with its basic characteristics, the smart grid data transmission system should have the following attributes.

1) Low power consumption and massive connection characteristics to facilitate massive deployment in the area and long-term reliable operation in battery-powered scenarios.
2) Complete the perception layer security functions such as physical data security, trusted service management, security upgrade management, and key life cycle management.
3) A complete network layer security solution adopts a unified communication system to facilitate unified deployment on a global scale and has a complete IoT card security management chain.
4) Access stratum (AS) and non-access stratum (NAS) network layer security features.

3 OVERALL TECHNICAL FRAMEWORK

NB-IoT is a new and streamlined IoT terminal communication technology proposed by 3 GPP R13 on the basis of long-term evolution (LTE) technology. It is a narrowband wireless cellular communication technology specially designed for the IoT to achieve the requirements of large connection, wide coverage, low power consumption, etc. From the perspective of basic features and network layer security features, NB-IoT highly matches the needs of the demand side in the smart grid. The basic characteristics of NB-IoT can be summarized as follows.

1) Deep coverage.

NB-IoT provides better deep coverage than other competing technologies. It has a high transmit power spectral density (PSD). In the downlink standalone mode, PSD is 43 dBm/180 kHz, which is 17 dB higher than that of LTE; in the in-band mode, PSD is 35 dBm/180 kHz, which is 9 dB higher than LTE. A multiple retransmission technology is employed to increase hybrid automatic repeat request (HARQ) gain and exchange coverage gain at a lower rate, and the maximum downlink retransmission and uplink retransmission are 2,048 and 128 times, respectively. In general, the coverage radius of NB-IoT is about 4 times that of GSM/LTE (Ratasuk et al., 2016; Martinez et al., 2019).

2) Ultralow power consumption.

NB-IoT has a power saving mode (PSM) and an extended discontinuous reception (eDRX) mode, which greatly reduce the power consumption of the module. In the PSM, the terminal is still registered on the network but cannot obtain the signal, so the terminal maintains a long time of deep sleep to save power. In the eDRX mode, the idle mode discontinuous reception cycle ranges from seconds to hours, and the connection mode discontinuous reception cycle supports 5.12 and 10.24 s, which greatly improves the downlink reachability during a low-power operation. Ultralow power consumption can ensure that a battery-powered NB-IoT terminal has a long service life of up to 10 years (depending on the specific application) (Wang et al., 2017; Kanj et al., 2020).

3) Ultralow cost.

By simplifying the protocol stack, the radio frequency circuit, and the complexity of baseband processing, NB-IoT does not require a duplexer, so out-of-band and blocking indicators are reduced. For example, it reduces baseband complexity and radio frequency circuits by 10% and 65%, respectively (Hoglund et al., 2020; Ballerini et al., 2020; Li et al., 2017). At present, the cost of NB-IoT modules has fallen below 15 yuan.

4) Massive connections.

NB-IoT adopts the narrowband technology and upper/lower equivalent power enhancement technology, thereby greatly increasing the channel capacity. NB-IoT improves spectral density by reducing the signaling overhead of the air interface. Through the optimization of the base station and the core network, NB-IoT realizes independent admission congestion control, downlink data buffering, and terminal context storage, which can achieve 50,000 connections/cell (Zayas et al., 2017; Sultania et al., 2020).

In terms of network layer security, NB-IoT has the following characteristics:

1) For terminals that support both the control plane optimized transmission scheme and the user plane optimized transmission scheme, NB-IoT adopts two layers of security mechanisms: AS and NAS. The former ensures Radio Resource Control (RRC) security and user plane security in the access network. The latter ensures NAS security in Evolved Packet Core (EPC).
2) By defining access safe management entity (ASME), NB-IoT realizes that the access network receives the highest level key from a home subscriber server (HSS). In addition, NB-IoT constructs a four-layer key structure, including terminal and HSS shared keys, terminal and ASME shared keys, terminal and mobility management entity (MME) shared keys, and terminal and base station shared keys.
3) The security activation of the access layer and the non-access layer is completed through security mode control (SMC), and the security of the access layer can be reactivated through the RRC connection re-establishment process and the RRC connection recovery process.
4) By using the integrity protection key and integrity check code (consisting of count value, bearer identification, upstream and downstream direction indication, and data content), a data integrity protection mechanism is constructed to ensure data integrity (Lu et al., 2020).

The basic characteristics and network layer security characteristics of NB-IoT show that it has the ability for large-scale deployment in the demand side of the smart grid. However, the basic characteristics of the energy IoT, such as the large number of nodes, many application scenarios, fast iteration speed, and constant risks of security upgrade, also put forward strict security requirements for NB-IoT module hardware, module software, and IoT card management.

Focusing on the secure transmission and intelligent analysis of massive data on the demand side of the smart grid and based on application scenarios such as a distributing substation, distributed power source, distributed energy storage, industrial electricity supply, and residential electricity supply, this study constructs a technical framework of “5G NB-IoT + Smart Grids,” as shown in **Figure 2**. The framework includes data secure transmission, trusted service management of data transmission, and the intelligent analysis of demand-side data based on machine learning. The technical details of the three aspects will be described in detail in the following sections.

4 SECURE TRANSMISSION SYSTEM

The smart grid demand-side data secure transmission system consists of two parts, the NB-IoT encrypted data terminal and the data transmission management system. As shown in **Figure 3**, the NB-IoT smart grid encrypted data terminal hardware takes the NB-IoT security module as the core, supplemented by peripheral circuits such as data acquisition and power management. The NB-IoT smart grid data transmission system is composed of a smart grid data terminal on the demand side, an NB-IoT base station of a telecom operator, a smart grid data server and application server, as well as a visualization platform, a Web client, and a mobile app, as shown in **Figure 4**.

The core of the smart grid demand-side data secure transmission system lies in the NB-IoT security module, which consists of the highly integrated SoC of NB-IoT R16/R17, SE-SIM (ESAM), and SE-SIM (eSIM). The software of the NB-IoT security module consists of AES/3DES, SDK software, RTOS software, eSIM application software, and eSIM OS. Among these, Advanced Encryption Standard (AES) and triple data encryption standard (3DES) are two standards in present data encryption. AES is a new encryption using an alternative replacement network, while 3DES is only an adaptation of the old DES encryption relying on a balanced Feistel network.

5 TRUSTED SERVICE MANAGEMENT PLATFORM

The main function of the trusted service management platform is to provide cloud management services for data secure

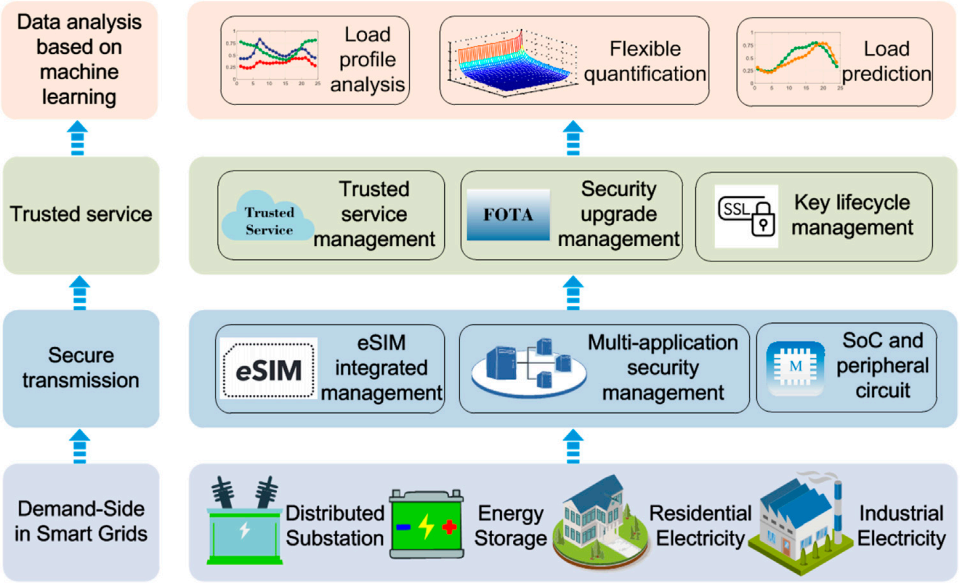


FIGURE 2 | Overall technical framework of secure transmission and intelligent analysis of demand-side data in smart grids based on NB-IoT.

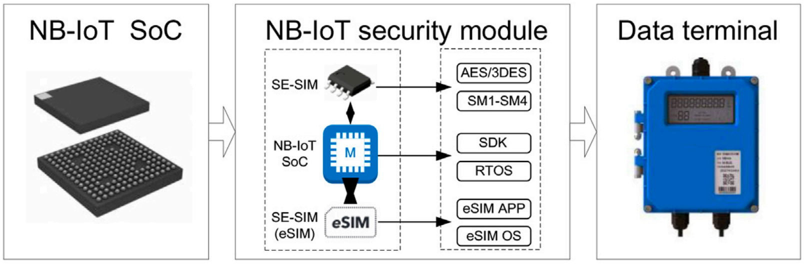


FIGURE 3 | Hardware structure of the NB-IoT encrypted data terminal.

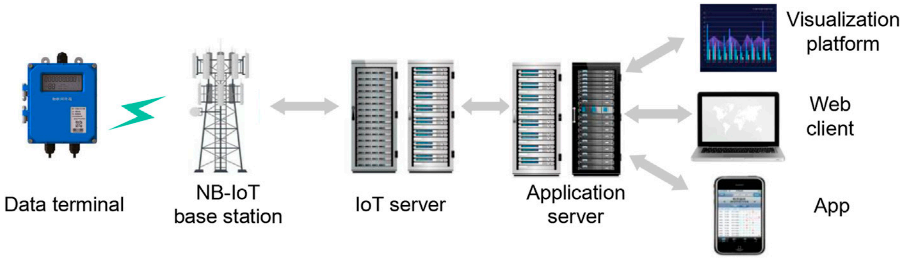
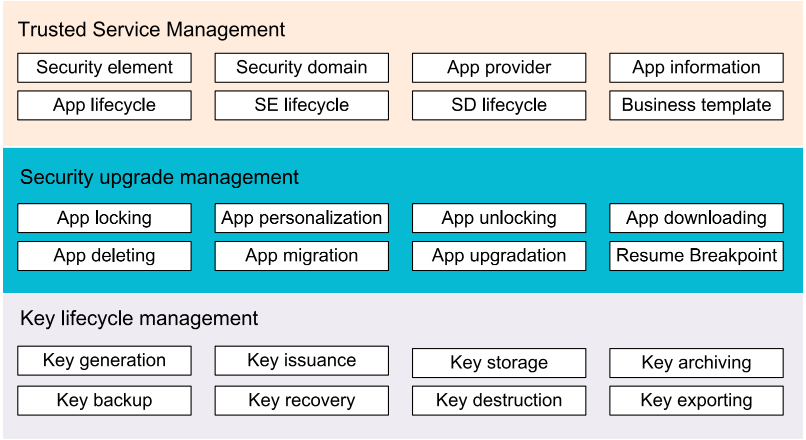


FIGURE 4 | Structure of a secure transmission system.

transmission systems in the demand side of the smart grid. Its core technologies include trusted service management, security upgrade management, and key lifecycle management, as shown in **Figure 5**.

1) Trusted service management.

Trusted service management is the top level of the whole platform. It is mainly responsible for the function management of the entire platform, including security element management, security domain management, application provider management, application information management, application lifecycle management, security element (SE) life



Trusted Service Management

Security element | Security domain | App provider | App information
App lifecycle | SE lifecycle | SD lifecycle | Business template

Security upgrade management

App locking | App personalization | App unlocking | App downloading
App deleting | App migration | App upgradation | Resume Breakpoint

Key lifecycle management

Key generation | Key issuance | Key storage | Key archiving
Key backup | Key recovery | Key destruction | Key exporting

FIGURE 5 | Structure of a trusted service management.

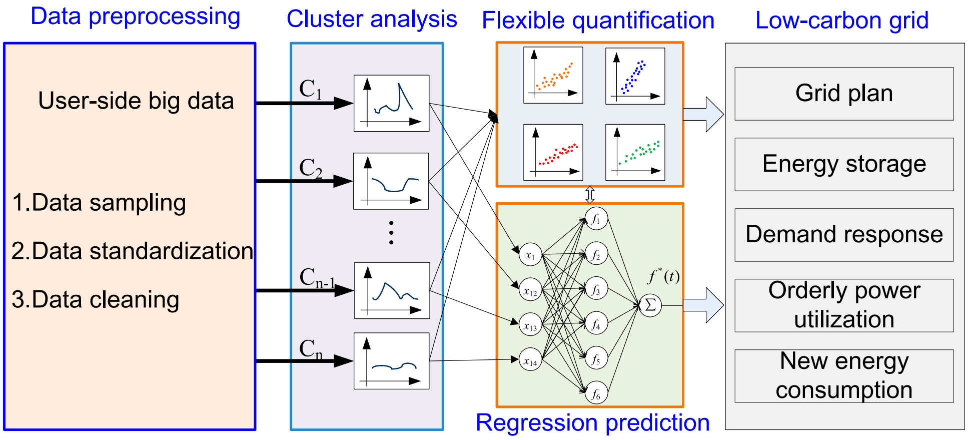


FIGURE 6 | Framework work of data intelligent analysis based on machine learning.

management, security domain (SD) lifecycle management, and business template management.

2) Security upgrade management.

If the software code of the data terminal needs to be upgraded due to functional changes, bug corrections, version updates, and other reasons, the safety of the upgrade process must be ensured. Security upgrade management mainly includes application locking, application personalization, application unlocking, application downloading, application deleting, application migration, application upgradation, and resume breakpoint.

3) Key lifecycle management.

The lifecycle management of keys is a necessary means to ensure data security. The key lifecycle management system includes key generation, key issuance, key storage, key archiving, key backup, key recovery, key destruction, and key exporting.

6 DATA INTELLIGENT ANALYSIS

The overall structure of the demand-side data intelligent analysis system is shown in **Figure 6**. First, pre-processing operations such as sampling, data standardization, and data cleaning are performed on massive data. Then the user load pattern is determined through cluster analysis. On this basis, demand-side flexibility is quantitatively analyzed, and regression prediction is performed on the grid load. The analysis results will serve for grid planning, demand response, new energy consumption, etc.

1) Cluster analysis of daily load.

According to different electricity consumption habits, the load on the demand side presents diverse characteristics. The daily load curve at a specific time interval can be used as the clustering feature. Taking 24 typical load characteristics in different seasons as clustering objectives, the user load characteristics can be curved through cluster analysis.

Assuming that the daily load curve of user *i* at hour intervals is $\mathbf{R}_{\mathrm{i}}$, a 24-dimensional vector is obtained after normalization, and the Euclidean distance between the daily load data of user *i* and the typical load characteristic *j* is

$$d\left(\mathbf{R}_{\mathrm{i}}, \mathbf{R}_{\mathrm{j}}\right) = \sqrt{\sum_{t=1}^{24} \left(R_{\mathrm{it}} - R_{\mathrm{jt}}\right)^2}, \quad (1)$$

where R_{it} and R_{jt} are the loads at *t* hours of user *i* and of the typical load characteristic *j*, respectively. The clustering objective function is the sum of the squares of minimum errors of *k* clusters, that is,

$$E = \sum_{i=1}^{k} \sum_{R\in C_{\mathrm{i}}} d^2\left(\mathbf{R}, \mu\left(C_{\mathrm{i}}\right)\right), \quad (2)$$

where, $\mu(C_{\mathrm{i}})$ is the cluster center of C_{i}.

2) Demand-side flexible evaluation.

According to the clustering results of daily load characteristics, through the evaluation of the user's removable and adjustable load, the demand-side flexible quantitative evaluation can be realized (Yuan et al., 2020; Yuan et al., 2021). The daily peak contribution of user *i* on the *j*th month is defined as

$$F_{\mathrm{i,j}} = \frac{1}{n} \sum_{d=1}^{n} \frac{p_{\mathrm{i,j}}^{d}\left(t_{\mathrm{d}}\right)}{P_{\mathrm{j}}^{d}\left(t_{\mathrm{d}}\right)}, \quad (3)$$

where $p_{\mathrm{i,j}}^{d}(t_{\mathrm{d}})$ is the power demand of user *i* at time t_{d} on the *j*th day, t_{d} is the time of system peak demand on the *d*th day of *m*th month, and $P_{\mathrm{j}}^{d}(t_{\mathrm{d}})$ is the system peak demand at t_{d} (Yuan et al., 2020).

3) Regression forecasting of daily load.

Based on the demand-side flexible measurement evaluation results, combined with multi-user daily load characteristics, the neural network regression prediction model of the time series of the daily load can be constructed. The inputs of this model are season, time, demand-side flexibility, user-side demand management, and energy storage ratio.

7 CONCLUSION

Essentially, the smart grid is an IOT-enabled application that allows utilities and their customers to exchange electricity and information and thereby improves energy efficiency. On the demand side, the value of IoT will be more prominent, due to the features such as a large number of nodes, many application scenarios, fast iteration speed, and emerging security upgrade risks. The rapid development of 5G communication technology will provide new power for the development of the smart grid. As the main technology of 5G mMTC, NB-IoT highly matches the needs of the demand side in the smart grid. Currently, the advantages of NB-IoT LPWAN in the demand side of the smart grid have not yet emerged, the issue of information security transmission has not been paid enough attention to, the value of demand-side data has not been fully tapped. Based on the aforementioned reasons, we constructed an all-round solution which consists of encrypted data terminals, management systems, and intelligent analysis methods. The main contributions of this study are as follows:

1) We analyzed the basic features of the next-generation demand side in the smart grid, the requirements of the data transmission system, and the basic features and network layer security features of NB-IoT. We also revealed that NB-IoT has the ability for large-scale deployment in the demand side of the smart grid.
2) We constructed the "5G NB-IoT + Smart Grids" technical framework from aspects of data secure transmission, trusted service management of data transmission, and the intelligent analysis of demand-side data based on machine learning and provided the technical details of the aforementioned three aspects in detail.

This research will contribute to the implementation of new generation information technologies on the smart grid, build a "5G + smart grid" in-depth integration application scenario, improve the intelligence of the grids, and further promote the "dual carbon" goal in power systems.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

Conceptualization, methodology, and writing—original draft: YS; writing, data curation, formal analysis, and visualization: TH; writing—review and editing: QW; resources: JZ; and resources and funding acquisition: YW.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the support of the National Natural Science Foundation of China (Grant Nos 61803345, 51807013, and 52177068); Science and Technology Development Project of Henan Province (222102240005); and Science and Technology Innovation Team in Universities of Henan Province (22IRTSTHN017).

REFERENCES

Abdallah, A., and Shen, X. (2015). Lightweight Security and Privacy Preserving Scheme for Smart Grid Customer-Side Networks[J]. *IEEE Trans. Smart Grid* 99, 1.doi:10.1109/tsg.2015.2463742

Ballerini, M., Polonelli, T., Brunelli, D., Magno, M., and Benini, L. (2020). NB-IoT versus LoRaWAN: An Experimental Evaluation for Industrial Applications. *IEEE Trans. Ind. Inf.* 16 (12), 7802–7811. doi:10.1109/tii.2020.2987423

Chen, Z., and Wu, L. (2013). Residential Appliance DR Energy Management with Electric Privacy Protection by Online Stochastic Optimization. *IEEE Trans. Smart Grid* 4 (4), 1861–1869. doi:10.1109/tsg.2013.2256803

Hoglund, A., Medina-Acosta, G. A., Veedu, S. N. K., Liberg, O., Tirronen, T., Yavuz, E. A., et al. (2020). 3GPP Release-16 Preconfigured Uplink Resources for LTE-M and NB-IoT. *IEEE Comm. Stand. Mag.* 4 (2), 50–56. doi:10.1109/mcomstd.001.2000003

IIOT Power (2019). *The Dark Side of the Smart Grid"*. Available from: https://www.powermag.com/the-dark-side-of-the-smart-grid/.

Jokar, P., Nicanfar, H., and Leung, V. C. M. Specification-based Intrusion Detection for Home Area Networks in Smart Grids[C]. Proceeding of the IEEE Third International Conference on Smart Grid Communications, Oct. 2011, Brussels, Belgium, IEEE, 2011:208–213.

Kanj, M., Savaux, V., and Le Guen, M. (2020). A Tutorial on NB-IoT Physical Layer Design[J]. *IEEE Commun. Surv. Tutor.* 22:2408-2446. doi:10.1109/comst.2020.3022751

Lang, A., Wang, Y., Feng, C., Stai, E., and Hug, G. (2022). Data Aggregation Point Placement for Smart Meters in the Smart Grid. *IEEE Trans. Smart Grid* 13, 541–554. doi:10.1109/TSG.2021.3119904

Li, Y., Cheng, X., Cao, Y., Wang, D., and Yang, L. (2017). Smart Choice for the Smart Grid: Narrowband Internet of Things (NB-IoT)[J]. *IEEE Internet Things J.* 5 (3), 1505–1515. doi:10.1109/jiot.2017.2781251

Lu, R., Liang, X., and Li, X. (2012). EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications. *IEEE Trans. Parallel Distrib. Syst.* 23 (9), 1621–1631. doi:10.1109/tpds.2012.86

Lu, T., Fang, H., Yuan, Y., Dai, B., and Sha, X. (2020). *The Evolution of NB-IoT Protocols—The Road to 5G IoT from R13 to R16[M]*. Beijing: People Post Press, 07.

Martinez, B., Adelantado, F., Bartoli, A., and Vilajosana, X. (2019). Exploring the Performance Boundaries of NB-IoT. *IEEE Internet Things J.* 6 (3), 5702–5712. doi:10.1109/jiot.2019.2904799

Nicanfar, H., Jokar, P., and Leung, V. C. M. (2012). Efficient Authentication and Key Management for the Home Area Network[C]. Proceeding of the IEEE International Conference on Communications, June 2012, Ottawa, ON, Canada, IEEE, 878–882.

Ratasuk, R., Vejlgaard, B., Mangalvedhe, N., and Ghosh, A. (2016). NB-IoT System for M2M Communication[C]. Proceeding of the 2016 IEEE wireless communications and networking conference, April 2016, Doha, Qatar, IEEE, 1–5.

Sanduleac, M., and Ciornei, I. (2021). High Reporting Rate Smart Metering Data for Enhanced Grid Monitoring and Services for Energy Communities[J]. *IEEE Trans. Industrial Inf.* 18:4039-4048. Accepted. doi:10.1109/tii.2021.3095101

Sultania, A. K., Mahfoudhi, F., and Famaey, J. (2020). Real-Time Demand Response Using NB-IoT. *IEEE Internet Things J.* 7 (12), 11863–11872. doi:10.1109/jiot.2020.3004390

Tan, O., Gunduz, D., and Poor, H. V. (2013). Increasing Smart Meter Privacy through Energy Harvesting and Storage Devices. *IEEE J. Sel. Areas Commun.* 3l (7), 133 1–1341. doi:10.1109/jsac.2013.130715

Trans-European Networks for Energy (2017). *Smart Grid Regional Group"*. Available from: https://ec.europa.eu/energy/topics/infrastructure/projects-common-interest/regional-groups-and-their-role/smart-grid-regional-group_en.

Wang, Y. P. E., Lin, X., Adhikary, A., Grovlen, A., Sui, Y., Blankenship, Y., et al. (2017). A Primer on 3GPP Narrowband Internet of Things[J]. *IEEE Commun. Mag.* 55 (3), 17–123. doi:10.1109/mcom.2017.1600510cm

Xu, X., Xu, Y., Wang, M. H., Li, J., Xu, Z., Chai, S., et al. (2020a). Data-driven Game-Based Pricing for Sharing Rooftop Photovoltaic Generation and Energy Storage in the Residential Building Cluster under Uncertainties[J]. *IEEE Trans. Industrial Inf.* 17 (7), 4480–4491.doi:10.1109/tii.2020.3016336

Xu, X., Jia, Y., Xu, Y., Xu, Z., Chai, S., and Lai, C. S. (2020b). A Multi-Agent Reinforcement Learning-Based Data-Driven Method for Home Energy Management. *IEEE Trans. Smart Grid* 11 (4), 3201–3211. doi:10.1109/tsg.2020.2971427

Yuan, Y., Dehghanpour, K., Bu, F., and Wang, Z. (2020). A Data-Driven Customer Segmentation Strategy Based on Contribution to System Peak Demand. *IEEE Trans. Power Syst.* 35 (5), 4026–4035. doi:10.1109/tpwrs.2020.2979943

Yuan, Y., and Wang, Z. (2021). Mining Smart Meter Data to Enhance Distribution Grid Observability for Behind-The-Meter Load Control: Significantly Improving System Situational Awareness and Providing Valuable Insights. *IEEE Electrific. Mag.* 9 (3), 92–103. doi:10.1109/mele.2021.3093636

Zayas, A. D., and Merino, P. (2017).The 3GPP NB-IoT System Architecture for the Internet of Things[C]. Proceeding of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops), May 2017, Paris, France. IEEE, 277–282.

Conflict of Interest: Author JZ is employed by Pinggao Group Intelligent Power Technology Co., Ltd.

The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.