# Power Industry Big Data Privacy Protection Processing Method Based on Fuzzy Logic and Intelligent Clustering

Feilu Hang*, Linjiang Xie, Zhenhong Zhang,
Wei Guo and Hanruo Li

*Information Center of Yunnan Power Grid Co., Ltd, Yunnan 650000, China*
*E-mail: feiluhang123@outlook.com; xielinjiang2021@163.com;*
*xiamenng163@163.com; gong2011yu@163.com; luvshinhwa@163.com*
**Corresponding Author*

Received 10 December 2021; Accepted 20 January 2022;
Publication 24 June 2022

## Abstract

The power industry is the corporate globe's backbone, delivering vital energy to industrial, manufacturing, promotional, and residential clients worldwide. Investment has been prompted by the shift of fuel and energy sources, rising environmental laws, and an ageing generating fleet and transmission infrastructure in industrialized nations with mature power systems. The evolving requirement in the power industry is causing several workforce challenges, including massive shifts in skills required, a skills gap for delivering. Performing newer technologies, changes occur when the Industry is experiencing high retirements and challenges recruiting a strengthening workforce. In this paper, Big Data based on the fuzzy logic method has been suggested to protect sensitive information. BD-FLM proposes a large data clustering-based privacy preservation probabilistic model that aims to cause the least disruption while maintaining the greatest amount of privacy. To alter or generalize sensitive data, use a methodology that secures sensitive information after detecting sensitive data clusters. In terms of conventional performance

*Distributed Generation & Alternative Energy Journal, Vol. 37_5,* 1461–1492.
doi: 10.13052/dgaej2156-3306.3758

assessment metrics, the model's privacy protection of individual data in large data with little disruption and effective reconstruction underlines its importance. This paper can automatically cluster based on the power characteristic factor and efficiently identify the power-related aspects of distinct user groups. The simulation results demonstrate that the proposed technique outperforms the comparison algorithm regarding prediction accuracy. As a result of anticipating the accurate values, individual privacy is preserved, but data accuracy is improved.

**Keywords:** Power industry, big data, fuzzy logic method, privacy protection.

## 1 Introduction of Big Data based on the Fuzzy Logic Method

Data are created and developed at an unparalleled pace, exceeding Moore's law, every day from various sources such as retail transactions, social media, and sensors are all possible. Even in everyday lives, consumers use search engines, e-mails, and messages to send and receive, social media networks to celebrate the infants, and GPS navigation systems to guide automobiles [1]. With this impact on day-to-day lives, scientific advancements and even government planning and policies have been changed by big data. In addition, other attributes like worth and truthfulness are usually taken into account [2]. Other systems, like Twitter, have overcome many of the shortcomings of GFT. Analyzing many tumours may uncover trends that help with diagnostic and treatment decisions regarding medical. Sensors and retail transactions are among the many sources of daily data that can generate huge amounts. Search engines, e-mails, social media networks, and GPS navigation systems are all being used to mark the birth of a child. Logic, defined as fuzzy, can contain truth values for variables in any real number between 0 and 1 since it is a many-valued logic form. Partial truth is the key concept here. Following the consideration of all of the available information, fuzzy logic can be used to solve an issue [3]. It's no secret that big data is changing how statistics is done since it allows for collecting information on an almost universal scale rather than relying on tiny samples. This fact has benefited economic and management studies [4]. The use of mobile privacy protection to deduce a person's socioeconomic class and accurately rebuild the wealth distribution across a country has been shown. Big data research, it seems, necessitates the use of certain approaches and tools. With the appearance of big data, a new paradigm of scientific study has evolved [5, 6]. In this

model, the value chain of big data often includes several fundamental tasks such as data collection, analysis, and interpretation/visualization. Mathematical instruments, data analysis approaches, visualization tools, and granular computing technologies have all been examined to carry out these tasks effectively and efficiently [7]. Batch processing, stream processing, or a hybrid approach using the Lambda architecture are examples of these approaches used in big data applications. Nearly every facet of big data processing and application development is fraught with difficulties, both technical and non-technical [8]. The pace at which data is generated has beyond the ability to process is an obvious general technological issue. Enhancing data management and programming skills is critical to developing innovative and scalable methods for analyzing and comprehending big data sets with complicated structural layouts [9]. Another important subject in big data analysis is accessing and studying data without compromising privacy and confidentiality. Consumers and clients often unintentionally or purposefully provide business companies and governments with personal information [10]. Because the misuse of personal data may compromise this autonomy, we suggest that policy emphasize how big data is utilized rather than how it is acquired and processed in this study [11]. Regardless of inflation, research expenditures remain stagnant, or dropping in real terms is a typical non-technical difficulty. Various solutions are being attempted to provide many different approaches to present difficulties. It has become an interesting and realistic methodology for the Supply chain to use methods such as the generalizations of fuzzy sets and fuzzy logic [12, 13]. In recent years, fuzzy sets have found use in a wide range of fields, including control and pattern recognition systems, machine learning, and artificial intelligence. Fuzzy set approaches in the energy sector may effectively safeguard individual privacy from prying eyes. Uncertainty management can take many forms. Extreme precision might lead to solutions that are either too costly or useless. Some distance from the situation may be required to unearth relevant data and make solutions possible. An advertising campaign should consider the preferences of the target audience. In other cases, though, it isn't necessary to distinguish between people's particular preferences. Fuzzy sets allow us to represent and analyze data at various granularity levels. Fuzzy sets have been used to handle and comprehend massive data in several contributions so far. Fuzzy set approaches have some potential or have already shown some benefits in the setting of large data for at least four reasons: Big data processing introduces uncertainty at every stage, not just in the data itself [14, 15]. For example, defective sensors or clients who aren't well-informed might

generate collected data, and the results of artificially intelligent algorithms may include uncertainties. In these situations, fuzzy set approaches might be an effective tool for handling privacy protection in the energy industry. Uncertainty management comes in a variety of forms [16]. Overly exact solutions to problems might be prohibitively costly or not be needed at all. A certain amount of detachment may be enough to unearth necessary information and propose answers. The buying preferences should be considered while establishing an advertising campaign. Various sources, such as retail transactions, social media, and sensing devices, generate enormous data daily. Search engines, e-mails and texts, social media networks, and GPS navigation systems are all used to celebrate the arrival of a new child. Consideration is generally given to factors such as value and honesty. However, it isn't always required to distinguish between people's particular preferences. In this situation, mining preferences from communities' points of view rather than individuals might be more efficient [17, 18]. Strategies such as fuzzy or rough sets, neural networks, and others that capture and handle information granularity will be more effective if used in addition to probability and rough sets for making decisions. Information granules, rather than numbers, are now widely accepted as the preferred method of communicating in systems and platforms with users. To interact with people in a manner that's clear and easy to understand, fuzzy set approaches such as com- putting with words might be useful [19, 20]. Fuzzy sets may improve existing big data methodologies and relieve present big data issues, such as the 5Vs, by pre-processing data or rebuilding the problem at a certain granular level. Unlike other prominent big data techniques like deep learning. Fuzzy set methods serve as a methodology that provides a new strategy for information abstraction and knowledge representation [21]. The model's privacy protection of individual data in huge datasets with minimal disturbance and excellent reconstruction highlights its value in terms of conventional performance metrics. In this study, the power characteristic factor can automatically cluster and identify the power-related characteristics of separate user groups. Fuzzy set techniques, which we'll see more of in the next sections, let us deal with data in a novel way. Because of this, we do not expect to solve large data challenges on utilizing largely privacy protection approaches. Using fuzzy set techniques, this work attempts to evaluate the current state of large data processing comprehensively. This review's taxonomy is based on data from two sources [22]. First, consumers use fuzzy set approaches to explain which techniques have been used by classifying previous contributions [23]. When and why fuzzy set approaches are relevant are explained in the second taxonomy, which groups literature

based on specific large data concerns. As discussed in this research, fuzzy set approaches can alleviate or minimize some of the present privacy protection concerns in the power business. This presentation explores some of the possibilities that may arise in light of current trends and difficulties. The findings of this study may be useful in developing privacy protection strategies for the power industry's big data [24, 25]. Authentication gateways must be protected from unauthorized access. Strong authentication is one of the most typical reasons for data leaks. The Least Privilege Principle can be used in this situation. Utilizing the most recent anti-virus software and retrospective attack simulation is imperative.

The main contribution of this paper

- Designing the BD-FLM has been proposed to protect sensitive information and improve the privacy protections of the proposed systems.
- The proposed BD-FLM large data clustering-based privacy preservation probability model seeks to create the least disturbance while keeping the most privacy. The model's privacy protection of individual data in big data sets with little disruption and successful reconstruction underscores the model's value in addition to standard performance evaluation criteria.
- The numerical results have been performed based on the proposed method BD-FLM to achieve the security, throughput, data transmission rate, scalability rate, attack ratio, and low energy consumption rate compared to other methods.

The remaining section of this paper is as follows: Section 2 explores the literature survey and Section 3 demonstrates the proposed BD-FLM for privacy protection in the power industry. Section 4 expresses the results and discussion based on the existing method, and Section 5 concludes the paper.

## 2 Literature Work

The term "big data" refers to a collection of extremely vast and complicated data sets that are challenging to store in a computer's memory. Massive amounts of data pose significant hurdles in searching, classifying, and analyzing it. This research presents a fuzzy-based supervised classifier to manage the search, storage, and categorization of large amounts of data. We presented a Random Sampling Iterative Optimization in this classifier. Fuzzy c-Means (RSIO-FCM) clustering algorithm for dividing large data sets into smaller ones. This set of subsets is sufficient to deal with all large data instances

(object space). YinghaoGuo et al. [26] introduced the deep reinforcement learning algorithm-based federated learning algorithm (DRLA-FLA) for the Efficient and flexible management industry. This paper will use a federated learning strategy to provide an effective and adaptable management system for the Industrial Internet of Things (IIoT) powered by mobile edge computing (MEC). Computational access points perform computational operations on all devices in the considered IIoT networks (CAPs). Although resource allocation based on certain centralized techniques may enhance IIoT network performance, such a solution was hardly efficient nor flexible. It is necessary to alter three factors to deal with this problem: job offloading, bandwidth allocation, and transmit power. Normalized system costs may be kept to a minimum while communication costs can be minimized. Furthermore, simulation findings show that the proposed federated framework can manage IoT networks efficiently and flexibly.

Edgar Batista et al. [27] evaluated the privacy-preserving process mining (PPPM) for preserving individual privacy during process mining analysis. Finding, monitoring, and enhancing actual processes using corporate information system event logs are part of process mining. Due to expanding dependence on telecommunications and technologies of information and anticipated widespread adoption of the Internet of Things, vast numbers of events may be collected for analysis to improve system performance. This study contributes to a new field of process mining research called the privacy-by-design idea is used in Privacy-Preserving Process Mining (PPPM). These attacks combine well-known location-based attacks with pseudonym and encryption attacks to show that current solutions are vulnerable. Process mining solution based on PPPM that preserves privacy event distribution homogeneity defeated this assault. This solution minimizes data loss while protecting the privacy of people who appear in event logs. The trials used six real-world event logs, and the results suggest that this method works in real-world situations.

Zeinab Shahbazi et al. [28] suggested the blockchain machine learning-based food traceability system (BMLFTS) for tracing supply chains for perishable food. Improved food traceability was one must-have for the food production business and for extending the shelf life of its goods. With the advent of blockchain technology in the anti-counterfeiting industry, one of the newest uses for blockchain technology is tracking the provenance of food. In many food production systems, data accuracy, scalability, and readability are lacking. In the same way, the supply chain process was sophisticated and took a long time to process. Blockchain technology provides a new supply

chain traceability ontology to address these difficulties. Researchers have developed a food traceability system (BMLFTS) using blockchain, machine learning, and fuzzy logic for manipulating perishable goods. The system is built on top of the shelf life management system. The suggested solution uses blockchain technology to handle weight, evaporation, warehousing transactions, and shipment there is a delay in the distribution chain. ML's reach into food traceability may be shown with the data flow on the blockchain. Finally, precise and trustworthy data are utilized in the supply chain to extend the distributed goods' shelf life.

Rahatiqbal et al. [29] developed the Hierarchical Spatial-Temporal State Machine (HSTSM) to build effective smart cities and sustain contemporary civilizations. Big data has a tremendous influence. This article examines the significance of Big Data in contemporary life and the economy and this paper analyze the issues associated with its effective use. Big Data analytics have several computational intelligence approaches as tools. Combining Big Data with Computational Intelligence (CI) uncovered several areas in which creative solutions to real-world smart city challenges might be found. Hierarchical Spatial-Temporal State Machine (HSSM) would be a universally inspired biologically inspired modelling framework used to research intelligent mobility in smart cities (HSTSM). Various regulatory, protection, valuation, and commercialization consequences of Big Data, its uses, and deployment are discussed further. The use of Big Data Analytics (BDA) to extract useful information from big data is on the rise, and many enterprises are following suit. As a tool to increase operational efficiency, analytics, including the deployment and usage of BDA tools, is considered by businesses as having strategic potential, driving new income streams, and gaining competitive advantages over business rivals. On the other hand, different analytic applications need to be considered. As a result, firms must first understand the BDA ecosystem before investing in expensive BD technologies.

HaiWang et al. [30] described the Data volume and velocity exploding in the period of massive amounts of data, posing a challenge because of the intricate structures. Transactions online and offline, social networks, sensors, and daily activities provide data as a combination of these sources. The BD-FLM data preservation probabilistic model maintains as much privacy as feasible, using data clustering to maximize privacy while reducing interruption. An evaluation method and data encryption are employed as part of this solution to the challenge. Algorithms can be analyzed in terms of their performance regarding the system's workload by using an analytic evaluation.

Deterministic modelling is a sort of analytic evaluation that can be used. With the correct handling of big data, decision-making in numerous fields such as business, management, and government may become more informed, intelligent, and relevant. Big data management requires a new study paradigm, but big data methods need even more long-term inventive activities shortly. Big data processing may use more fuzzy sets as a result. Due to its ability to capture and quantify uncertainty, large-scale data processing has used fuzzy sets. Numerous cutting-edge ideas have been put forward under the Granular Computing framework. This paper may deduce from a few basic concepts. This paper emphasizes the possibility of a unique, promising processing environment provided by the more complex addition of new features to fuzzy sets and merging these features with others.

## 3 BD-FLM for Privacy Protection in Power Industry

Since numerous power sectors are quickly digitizing, bigdata variables play an important role in the power industry's data collection and processing paradigm. Firms may now create and provide robust industrial systems and services using big industrial data collected from many sources. MCS's crowd sensing services are unduly or improperly safeguarded, and their quality is poor due to the existing consistent privacy protection policy for all sensing data. Big data-based fuzzy logic has been proposed in this research to safeguard sensitive information for this reason. Although the BD-FLM data clustering-based privacy preservation probabilistic model tries to maintain maximal privacy, the disturbance is minimized. This approach is presented using an evaluation algorithm and data encryption. As soon as the level of privacy of a user's data is determined, evolutionary algorithms are used to develop an upload technique that makes sense given the data. An additional technique of data collection proposed in this article ensures privacy, accuracy, and timeliness of data while simultaneously assuring privacy, correctness, and timeliness. Several simulations based on real-world data and theoretical research paths indicate that BD-FLM is efficient and offers great privacy protection in the electricity business.

Figure 1 illustrates the components of the power industry protection system. Disruptions to a power system may be caused by natural occurrences including lightning, wind, trees, animals, or even by human mistakes or accidents. These can all impair the system's performance. Short circuits, overloads, and open circuits may all occur due to these types of disturbances in the system. Short circuits are of particular concern because of

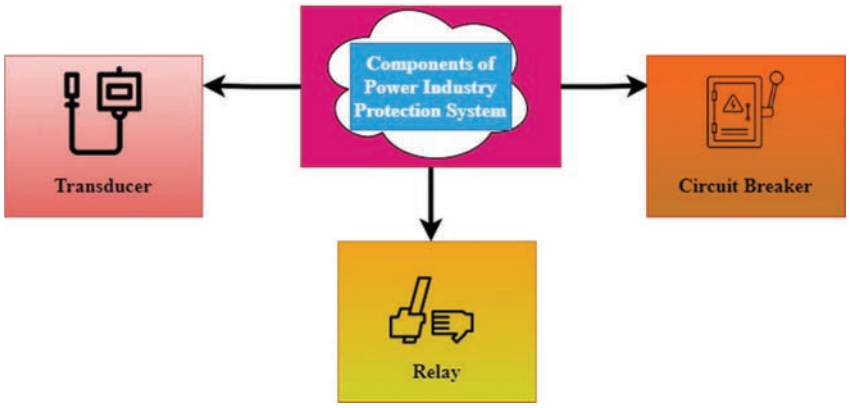


**Figure 1** Components of the power industry protection system.

the potential for equipment or system element damage and other operational issues, including voltage dips, frequency decreases, synchronism loss, and full system collapse. A device or set of devices is thus required that can detect a disturbance and immediately respond to relieve any negative effects on the system element or the operator is required. Protective systems are built to automatically disconnect faulty system elements when short circuit currents are high enough to put them or the whole system at risk. An alert will go off if the defect causes overloads or short-circuit currents that aren't dangerous right away, and the protection system may correct the issue. A security system comprises three main parts: Circuit breaker, protective relay, and transducer the following paragraphs provide a quick overview of these elements. If there are abnormalities in the system, the transducer can sense them and decrease the excessive short-circuit current and voltage levels. CT windings might be damaged by almost ten times the typical short-circuit current under fault circumstances. Transformers have a single-turn main winding and a multiple-turn secondary winding. Open-circuiting, the secondary of a CT, is dangerous while the main is powered. The transformer's secondary voltage is set at 120 volts, the industry norm. The PT is a two-winding voltage transformer like any other in low-voltage applications. A capacitor voltage-divider circuit is used with the PT for high- and extra-high-voltage primary voltages. The capacitors are linked in series, and this creates the main voltage. It is possible to measure a few kilovolts across a lesser capacitance value capacitor using a PT transducer. In a protective relay, the signals produced by the transducers are processed by the device, which may be either a current or a voltage, or both. These signals may be produced by short circuits, faulty equipment

or lines, lightning strikes, or surges. The safety relay may sound an alert or start or open different interrupting devices. Protective relays may be divided into electromechanical and solid-state types depending on how they are constructed. This electromagnetic force or torque is utilized to physically open a series of contacts to allow or begin tripping circuit breakers using the electromechanical relay. The identical impulses activate an electromechanical relay's solid-state relay. However, the relay connections are not physically opened or closed. A solid-state device changes from conducting to non-conducting, simulating a relay contact switch. Solid-state relays are older than electromechanical relays. Electromechanical relays are still used in the majority of power system installations. Solid-state relays have become increasingly popular due to their increased dependability, adaptability, and quick reaction time. Solid-state relays have taken the place of certain electromechanical relays, and in modern installations, both kinds are common. When it comes to electrical circuits, circuit breakers are the mechanical devices utilized to activate and interrupt them. A few milliseconds should be enough for it to open and shut. It should carry the maximum rated current continuously at its nominal voltage. The circuit breaker's interrupting rating tells us how well it can interrupt a big short-circuit current. Circuit breakers have current-carrying contacts that, when opened, create an electric field across the contacts, ionizing the medium and causing an arc to form. The circuit breaker must extinguish this arc or stop as rapidly as possible.

Figure 2 shows the architecture of the proposed BD-FLM. It has been made possible by distributed storage to use the storage as a service model for large-scale remote data storage, which is now considered one of the most powerful cloud computing technologies. The cloud service paradigm has become a viable option because of the proliferation of big data and the

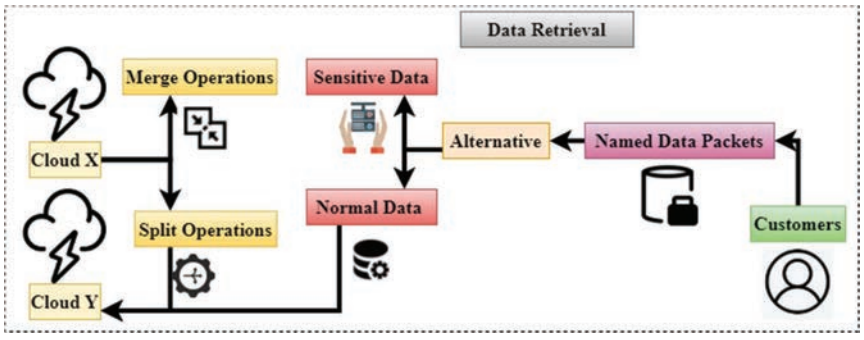


**Figure 2** The architecture of the proposed BD-FLM.

development of Web services and networks. A few examples of the various cloud storage service providers that have come up with attractive storage service packages that give consumers vast and scalable cloud storage spaces are Amazon, Dropbox, Google Drive, and Microsoft OneDrive, to name a few. However, security concerns stemming from cloud-based operations continue to impede the adoption of STaaS in organizations. There is considerable worry among cloud clients over data privacy and the security of the sensitive information they have committed to the cloud providers. Although various previous studies have addressed this matter, contemporary STaaS deployments are embarrassed by this issue, a source of contention for the industry. Aside from that, in recent years, researchers have looked at the use of Mass Distributed Storage (MDS) to improve the quantity of data available for Storage. In addition to high-level scalable computing performance. Developing techniques for securing scattered data storage is necessary since attacks might come from any direction. When data is kept undistributed, it is more vulnerable to more destructive attacks or abuse actions, such as a data transfer attack.

Due to the rules and regulations, unexpected activities are still conceivable on the cloud server-side. Meanwhile, power business factors make balancing utility and security requirements difficult. Therefore, securing distributed data in cloud systems is a challenging topic to handle since the risks originating at diverse network levels are only partly addressed. In this post, the author discusses cloud operators misusing difficulties and steps to prevent cloud users' information leakage from cloud servers. This paper provides a Big Data method based on the fuzzy logic technique for the security of personal information in the power business (BD-FLM). An alternative approach evaluates the user's data using algorithms for searching named-data-packets that may be used by the user. By using solid arrow lines, customers can see the splits and storage methods in action. The data retrieval operating directions may be identified and followed using broken arrow lines. All of the standard data will be stored on a single server in the cloud. This happens when sensitive data is split into two sections and sent to Cloud X and Cloud Y, two different cloud servers, for storage and processing. Adoption of the strategy this paper has recommended alternative data distribution is critical to the success of this approach. The secure, efficient data distributions method is used to partition data to prevent sensitive information from leaking to the cloud while utilizing the least resources possible. The proposed approach is noteworthy because it provides a flexible solution for organizations such as the power service industry that wish to use it. This paper needs a high level

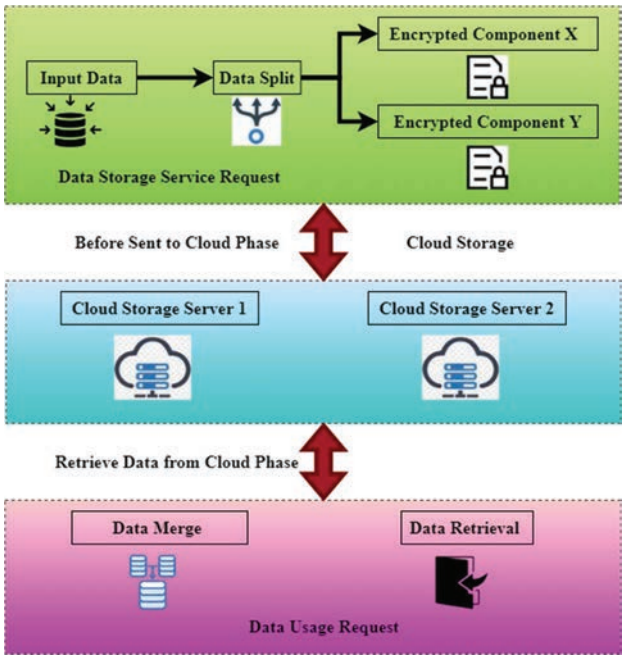


**Figure 3** Data distributed storage process splits data packet in BD-FLM.

of data storage security. This proposed approach is the most effective way to prevent cloud service providers from gaining direct access to users' original data and information.

Figure 3 explores the data distributed storage process that splits data packets in BD-FLM. An outline of D2SP's procedure inside the BD-FLM paradigm may be found right here. It demonstrates the fundamental method of privacy protection in the power industry. The model phases are indicated by the boxes in the centre and left corners of the figure. Currently, information is being processed to create two independent streams from one incoming one. These two steps are important to successfully transmitting data through a network. Data from the customer's input D is divided into two distinct components before being delivered to the cloud for processing. In contrast to the other one, which combines the data, this one will get the original information. As seen in the illustration, the letters X and Y are encrypted components. A few phases are involved in this technique, and they are as follows: Data C is created at random initially, and it is then utilized to generate additional data packets by performing the D-C operation on them.

It is necessary to save this key on the user's side in a dedicated register. Finally, the two encrypted data packets were transferred to two different cloud servers, one for decryption and one for storage, to complete the process. Data packets from both cloud providers must be sent to the data consumers during the retrieve data phase. After getting data from the cloud, it is necessary to do several procedures to return to the original data. The summarization of the corresponding data packets is required to create the new data string. The recovery of the original data will mark the conclusion of this process. The cloud computing security paradigm has been compromised from the network to the system management levels on practically every level gained access. Since technological applications, like Virtual Machines, are interconnected, many security issues in networks and data storage apply to cloud computing. To begin, cloud computing's data management security needs to protect the sector's overall security, implement encryption preparations or data classifications. It's a way to save money on computer resources while maintaining cloud-based information security. By categorizing data in various ranks and employing searchable encryption, users may determine whether or not data has to be safeguarded, for example. In contrast, current data management solutions are predicated on the assumption that cloud service providers would not mishandle the data in their possession. They would have only restricted access to it under their control. Essentially, this implies that the acts of cloud service providers are closely scrutinized. Depending on the conditions, it is possible to recover data even if it has been encrypted on the cloud's end. The monitoring and protection of data storage in the cloud is yet another component of cloud data security that considers data processing or activities in the cloud. Attribute-based encryption is a kind of encryption that may protect private information when data is transmitted across several clouds.

Figure 4 shows the big data processing using fuzzy set approaches. These tactics, which will be addressed in further detail later in this section, may be beneficial in processing enormous volumes of information. When used across the value chain, fuzzy set techniques may be used for anything from handling raw data uncertainties and annotations to creating granular data representations for artificial intelligence systems. The next parts of the paper provide an overview of the recently established fuzzy set techniques in the power industry, and Fuzzy set techniques can provide better outcomes in some particular big data applications. For example, the technique described in this article, which is based on the basic fuzzy rule-based system and fuzzy sets, is an excellent illustration of this. There are many ways in which our

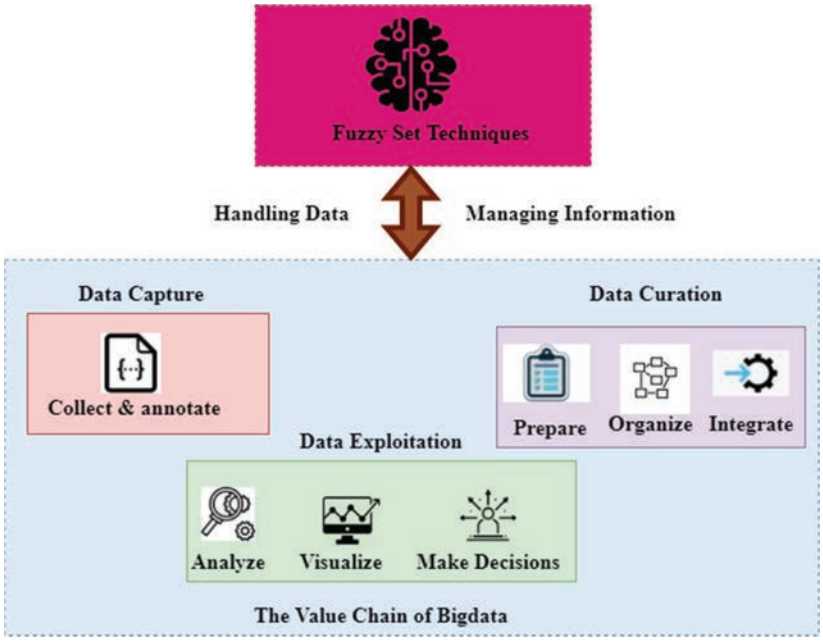


**Figure 4** Big data processing using fuzzy set approaches.

daily behaviours, online and offline transactions, social networks and sensors can all contribute to data growth. Medical research, health care, business, and government all benefit from maximizing the power of big data in their decision-making processes. Despite adopting a new research methodology, new ways of thinking about enormous data demand ongoing innovation. Because of their capacity to characterize and quantify uncertainty in data, fuzzy sets have been employed for large-scale data processing. To locate trillions of pieces of data swiftly and efficiently, fuzzy logic can be used. Reduced unnecessary data is another benefit of the Fuzzy logic approach. Because of its flexibility and ability to adapt to the user's needs, fuzzy logic has various advantages for data mining. Combining fuzzy and rough sets effectively solves problems involving vast amounts of data. Fuzzy rough sets were used for incremental feature selection and detection of power industry privacy for other purposes. Rough sets and FCM algorithms were used to develop the electricity sector separately. This paper developed a complicated decision-making system that depends on the fuzziness and coarseness of data and an algorithm for ranking orders based on how closely they match the ideal solution. Although their solution has been tested on real-world

massive data situations, it has not been proven effective. To understand the obligations of fuzzy set methods, the power sector must first recall a well-known paradigm for huge data processing: data-intensive research. This will allow them to grasp the responsibilities of fuzzy set approaches more readily. Instead of computers, data is the primary emphasis of the paradigm, which results in data-driven decision-making. This stage takes into consideration the annotation of data. It can perform a wide range of data curation operations, including data, organization, and integration. A wide variety of activities, from data preparation to analytic result presentation, are covered by Workflow Data Exploitation. Preserving the privacy of large amounts of data Method important enough to satisfy the requirements. Security of large amounts of cloud-based data poses various problems for firms who use it. Among these dangers include the theft of online data, malware, and DDoS assaults that can bring down a server. On-premises or cloud-based servers, where data is being stored, can be hacked or kept hostage, which is the second risk. Unauthorized access and theft of corporate data are two of the most common threats to the confidentiality and integrity of the company's data. For example, ransomware, which can encrypt or delete data, and other assaults that can corrupt or modify it are all included in this protection. The results may be presented as static documents or a software program that enables users to explore and enhance findings before receiving informative judgments.

In many large-scale data curation challenges, such as data clean, fuzzy set techniques, such as those proposed in this method, give a novel approach that is both efficient and effective. For example, the regular Statistical process was combined with a fuzzy set of rules and weights to form the fuzzy process, which resulted in better data quality. Fuzzy sets have been used to build new methods to deal with the authenticity of vast volumes of data. Other research projects are connected with data preparation, such as managing large datasets in a distributed environment. Using a linguistic word as ambiguous as possible, each level was represented by an image. Whenever a new work is established, only nodes with the same level as the job are permitted to participate in the bidding process. In this situation, fuzzy set techniques may aid in speeding up access to the information.

Figure 5 shows the relationship between big data, smart manufacturing systems (SMS), and product service systems (PSS). Industrial big data system Studies on industrial big data approaches, technologies, and systems from the standpoint of data flow are many. Data from all life areas reveal exponential expansion features due to the fast growth of communication, information, and

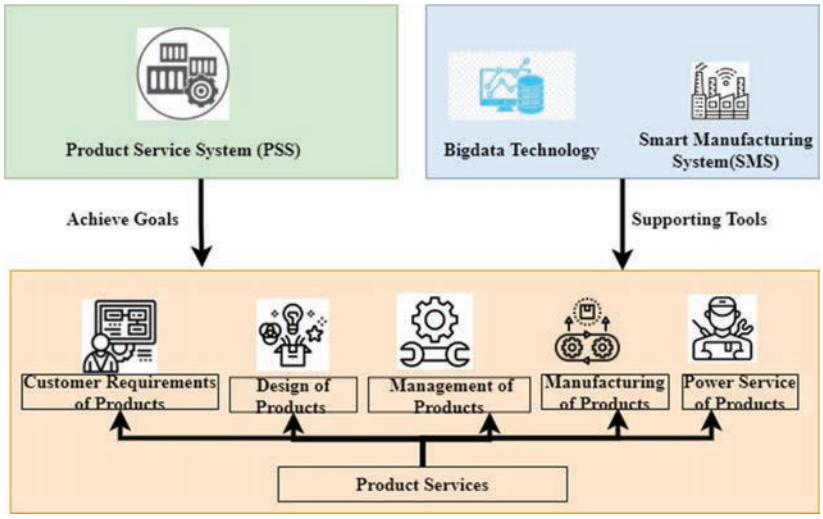


**Figure 5** The relationship between big data, smart manufacturing system (SMS), and product-service system (PSS).

internet-related technologies industry's use of big data is generating or consuming big industrial data as it spreads. As a tool to help the product-service system provide value for enterprises, a smart manufacturing system (SMS) connects services focused on the product life cycle. As a result, the power industry's system model is that massive amounts of data system engineering analysis were used to examine the application, and a generic reference model for big data was developed. A generic reference design for the big data power industry's implementation route was put forward. It was then recommended that a Big Data approach based on fuzzy logic be used to safeguard sensitive information about the influencing elements in the electricity sector. It may provide the power sector and government a theoretical foundation for developing, formulating, and implementing big data. But it may give some pointers on improving and extending the architecture for intelligent production. When evaluating large amounts of data, privacy and confidentiality must be considered. It is common for customers and clients to share their details voluntarily or inadvertently. We believe that regulation should focus on how big data is utilized rather than gathered and processed because misuse of personal data may jeopardize this individual's autonomy. A wide range of solutions is being sought to address the current challenges. The Supply Chain has found that fuzzy sets and fuzzy logic generalizations are fascinating and realistic.

Data-intensive modelling and predictive engineering are components of the smart manufacturing system (SMS). This novel product can boost the electric power industry's efficiency and profitability while reducing its environmental impact. This includes manufacturing processes and materials, manufacturing data, predictive engineering, sustainability, resource sharing, and networking. Smart manufacturing is the future state of manufacturing. A product-service system is a marketable collection of goods and services that work together to meet a user's requirement and have drawn the attention of global manufacturers to give high-value-added services. PSSs are becoming more popular. Product-service systems are a progression of current product development methodologies that combine services and product development approaches to achieve sustainable development. Today, product service system research encompasses everything from after-sale service to service focused on the whole product life cycle. Power industrial big data is necessary for achieving smart manufacturing in the energy industry, and smart manufacturing must embrace big data to be successful. Smart manufacturing may benefit from big industrial data by increasing the design, manufacturing, supply, and service accuracy, efficiency, predictability, and decision-making skills. It is considered smart manufacturing technology since it uses intelligent enabling technology inside the smart manufacturing system and has built-in privacy protection for power industrial big data. The intelligent and sustainable basis that supports the ubiquitous, secure, reliable, and capable of detecting the whole systemand assessment is a basic commonality. PowerIntelligent enabling technology, which includes big industrial data, is critical for advancing other technologies. In the power industry, big industrial data is a collection of interconnected data sets, the nucleus of the industrial internet, the primary raw material for intellectual development in the power sector, and a critical strategic resource for industrial transformation and upgrading.

Firstly, association rules are categorized according to their confidence value before being evaluated for these criteria. This paper used a static dataset for the previously specified factor (without new data entrance). So, formula (1) may be used to calculate the power industry privacy protection informationcriteria for selecting the best item(q).

$$\mathrm{PQ} = \frac{\sum_{i=1}^{n} \boldsymbol{m_i} \times \boldsymbol{x_i}}{\boldsymbol{m_j}} \tag{1}$$

Where PQ is the information most appropriate item selection and $m_i$ is the number of rules in which A is involved that have the same membership function, $\mathrm{m_j}$ is the total number of rules in which a participates, though each

member serves a distinct purpose, $x_i$ is there a difference in the amount of information lost when using various degrees of privacy protection.

Because of this element, the database has a static perspective, and the amount of information lost is determined. This item's difference in confidence values from other rules is examined for the second factor, but only up to a predetermined confidence level. The formula used to calculate this factor is as follows (2),

$$EFG = \sqrt{\sum_{j=1}^{n} (D_j - D_{R_j})^2} \tag{2}$$

Where $EFG$ is an imbalance between the levels of reliability, $D_j$ determines the degree to which the trust in a rule is justified. $D_{R_j}$ is a high confidence value. $n$ is the total number of rules in which a participates.

In each membership function, newly added data negatively influences the confidence value of the association rule, lowering it below a threshold. Because of this, it's necessary to calculate the difference in confidence values between association rules and the linked membership function minimum. If this number is higher, the chances of modifying the underlying membership function are reduced. Obviously, by using the current membership function for privacy protection, this paper aims to minimize the probability of the whole occurring. Finally, integrating the findings of PQ and $EFG$ values, but with suitable effective weights, as formula, may be used to choose the best item (3)

$$APU = \gamma_1 \times \mathrm{PQ} + \gamma_2 \times EFG \tag{3}$$

Where $APU$ is the possibility to choose the best item for privacy protection by selecting one with a lower best item-set value, $\gamma_1$ and $\gamma_2$ is the values of these effective weights are modifiable.

To be clear, the first element in a large dataset involves current data, and the second factor involves potential new admission data. Since the PQ factor focuses on current association rules, it seems more essential. In contrast, the EFG factor makes this decision more intelligent based on anticipated future data. The Transmitter allows the extraction of features from signals with arbitrary time-frequency resolution, includingthe power industry's stationary and non-stationary properties. The expression for signal $y(t)$ maybe written as

$$y(t) = \sum_{j-1}^{\beta} y_i^j(t) \tag{4}$$

Let $y(t)$ is the signal with a certain time delay,after decomposing the signal $y(t)$ into $i$ stages of decomposition and reconstructing the node signals as $y_i^j(t)$. The signal energy of the nodes $H_i^j$ maybe described as follows,

$$H_i^j = \int_{-\infty}^{\infty} y_i^j(t)^2 dt = \sum y_i^j(t)^2 \tag{5}$$

Where $H_i^j$ is the amount of energy that has been stored in the particular frequency spectrum. The Power transfer theory states that each node signal carries information about the original signal within a certain time-frequency range. When there is an irregularity in the original signal, the frequency components will undoubtedly change. As a result, studying the fluctuating pattern of $H_i^j$ may help discover problems. The measurement noise rapidly products power system components with modest energy magnitudes. As a result, in this article, the criteria for detection identification are developed as follows instead of examining individual node signal energies,

$$BGV = \sum_{j=1}^{n} \frac{|\nabla H_i^j - \nabla \overline{H_i^j}|}{\nabla \overline{H_i^j}} \tag{6}$$

Where $BGV$ are the privacy detection, $\nabla H_i^j$ is the node signal energy to total signal energy ratio and $\nabla \overline{H_i^j}$. Time-frequency node signal energies and the criteria BGV are affected by developmental problems in the signal. The node signal energy ratio is a reference baseline for evaluating future signals and determining the mean value of node signal energy. The first $n$ dominating nodes are kept to eliminate the impacts. Occurrences, however, are not the only thing that might alter the criteria; measurement disturbance can have an impact on it.

This technique relies on real data, which severely restricts its use in the large data sector despite its capacity to avoid noise interference and accomplish detection methods with high probability. Frequency modulation theory's limitations are overcome by compressive sensing theory, which simultaneously acquires and compresses data. The idea serves as a solid foundation for a large data defect detection technique that was recently suggested. The power protection $y \in K^M$ is stated as follows:

$$y = \sum_{j=1}^{M} \delta_j \sigma_j \quad \text{or} \quad y = \delta\sigma \tag{7}$$

Where $y$ power protection, $\delta$ is the binary transform basis for the $M \times M$ transformation, $\sigma$ is the binary basis's expansion coefficient vector. Compressive sensing theory says that a limited number of non-adaptive, linear measurements may be used to gather the power detection $y$. After then, it will be as follows:

$$y = \alpha_w = \alpha\delta\sigma \tag{8}$$

$$\widehat{\sigma} = \arg\max \|\sigma\|_{0,1} y = \delta\alpha\sigma \tag{9}$$

Where $\alpha$ is the random measurement M and the second random measurement matrix of size N. $\alpha\delta$ is the incoherence constraint was followed by a pair of power systems. $\sigma$ is the coefficients of expansion, $\|\sigma\|_{0,1}$. There are n nonzero components in, from this can count them as one norm.

## 4 Results and Discussion

One of the most important issues about adopting big data applications in the power distribution system is the possibility of poor quality data influencing decision-making without the operator's knowledge or consent. Therefore, a big data privacy protection processing method based on fuzzy logic and intelligent clustering (BD-FLM) for the power business is proposed in this study. Data purification procedures and state estimation applications may fail to detect serious sensor failures, resulting in this situation. Data security and privacy are key issues to be worried about. Using leaked interval meter data, it's easy to determine whether or not someone has an electric vehicle or a rooftop solar panel, or even what brand of appliance they're using if they're not at home, for example. The basic privacy assumption of "notice and consent" has been made outdated by the proliferation of the big data-based fuzzy logic method. To reduce consumer concerns about big data analytics, this paper must increase cyber-security while enacting new laws and regulations to protect the privacy of customers' data in the power sector.

### 4.1 Security Ratio (%)

If consumer security is not maintained when devices analyze and communicate enormous volumes of data, data collection, processing, and transmission may be compromised. To keep things safe, this paper needs both technical and legal means. Power industrial operations, such as manufacturing plants and protective control applications, rely on big data. Because of the systems'

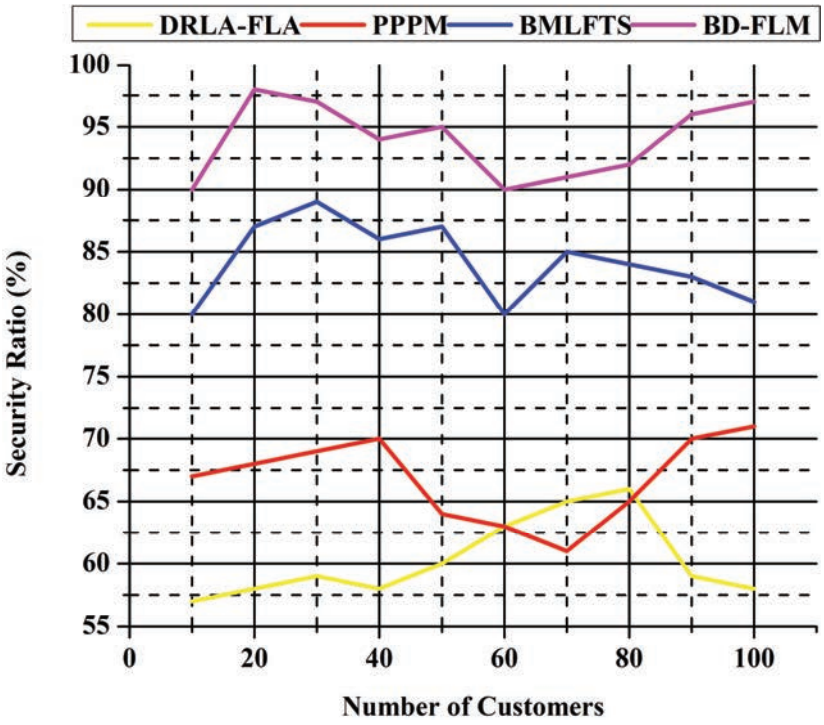


**Figure 6** Security ratio (%).

complexity, ensuring security and confidentiality in power industrial big data systems is tough. Security requirements definition and implementation are tough since they cannot be demonstrated. The protection of individual privacy may be improved by gathering and securely processing data. Even if all other attempts fail, devices may be prompted to verify their identity one last time without providing personal information. An in-depth study of various security methods and solutions has discovered security flaws and dangers. In light of the results, researchers now have new options to address some of the security issues generated by bigdata analysis in the electrical Industry. Figure 6 shows the security ratio (%).

### 4.2 Scalability Rate (%)

Most Internet of things does not allow the direct deployment of such solutions due to the high costs and resource demands of these operations and the restricted availability and scaleability of IoT devices. A computer-intensive

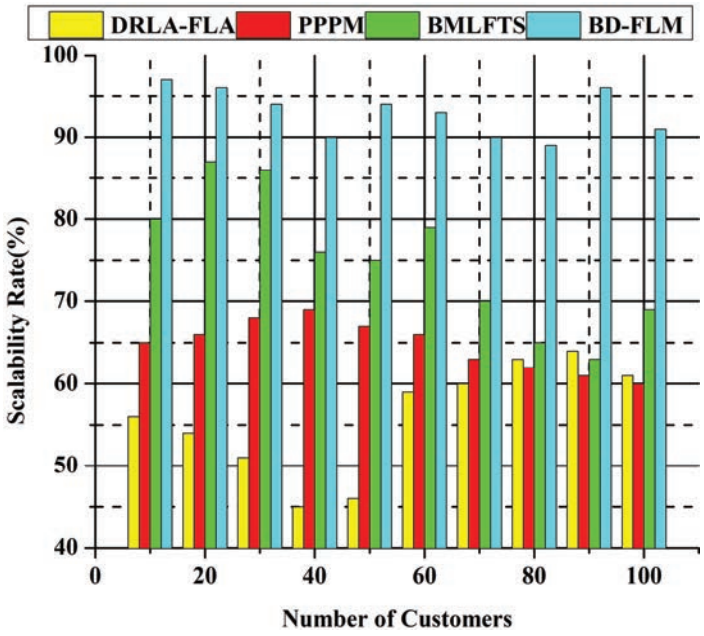


**Figure 7** Scalability rate (%).

process is employed with IoT applications to raise computing expenses despite asymmetrical key systems' minimal memory, great scalability, and attack resistance. Another issue with old methods is that they don't scale effectively, and security is no longer as important as delivery these days. This study uses computer-intensive methods that raise the computational costs for Internet of Things (IoT) applications because asymmetric key regions have minimal memory requirements, are highly scalable, and are resistant to threats. As a result of these initiatives, users may be certain that their data is completely private and secure. There are various benefits to be gained from this data integration, including reducing fragmentation in large distribution networks, the development of scalability, and the storing of financial data. The processing capacity and data latency are both problems with scalability that plague some public fuzzy networks. A side chain is added to the fuzzy to boost speed,and the system is optimized for cloud computing. Data security, secrecy, and the efficiency and scalability of edge node integration necessitate an architecture that protects them all. Cloud service providers provide cloud storage and authentication services to assure accurate, secure, scalable, and effective data storage. Figure 7 shows the scalability rate (%).

### 4.3 Attack Prevention Ratio (%)

Clients may be protected against man-in-the-middle attacks by implementing the user authentication method described in the article. This authentication method is difficult to duplicate since identifying the device (used in authentication) is produced by copying an unknown random quantity. When it comes to the authentication protocol, every contact with a customer, node, or gateway necessitates the use of three random numbers. As long as communication messages have been updated, numerous attempts will be thwarted. If an attacker has the device's identifier, they can still not decode the data packet because of the private key included in the data sets. Furthermore, the attacker can't pretend to be a reliable network since he doesn't have access to the pre-shared key. To send, receive, and manipulate the authentication process, attackers need several personal factors, including the secret Identities of the customer and the sensing equipment in question. Protection strategies are critical in such a setting, and data storage may aid by providing appropriate authentication procedures and hardware and software upgrading processes that boost security.

Consequently, only authorized users may access the network while everyone is shut out. Malicious individuals may take control of and access personal data without consent. Table 1 shows the attack prevention ratio (%).

**Table 1**

| Number of Customers | DRLA-FLA | PPPM | BMLFTS | BD-FLM |
|---|---|---|---|---|
| 10 | 56.2 | 60.5 | 70.9 | 90.4 |
| 20 | 54.0 | 65.0 | 71.0 | 98.0 |
| 30 | 56.0 | 67.0 | 73.9 | 97.6 |
| 40 | 58.0 | 67.0 | 75.0 | 94.0 |
| 50 | 59.5 | 68.0 | 78.0 | 96.9 |
| 60 | 58.0 | 68.9 | 79.0 | 97.9 |
| 70 | 52.0 | 67.8 | 80.9 | 93.8 |
| 80 | 51.0 | 64.0 | 89.7 | 96.0 |
| 90 | 59.0 | 66.9 | 90.1 | 95.0 |
| 100 | 58.7 | 60.8 | 92.8 | 97.9 |

### 4.4 Energy Consumption Rate (%)

Serious data devices consume a lot of power, which is a big problem. The power industry is hampered by energy requirements for big data analysis and technology, while many processes need vast energy to operate at full capacity.

Using efficient energy activities like clustering as a solution might be a good option. By sending data to adjacent cloud servers, clustering minimizes the need for processing, allowing big data devices to consume less energy. Data centres employ cloud networking to check for data duplication sporadically. Large computations are required when edge devices receive data requests from other devices, which increases big data's energy consumption. Articles like this take advantage of the internet's highest recognition and convolution to safely distribute labour while reducing industrial energy consumption. Table 2 shows the energy consumption rate (%). From this graph, it's easy to see that adopting the proposed strategy resulted in lower energy use.

**Table 2**

| Number of Customers | DRLA-FLA | PPPM | BMLFTS | BD-FLM |
|---|---|---|---|---|
| 10 | 70.9 | 69.0 | 59.0 | 29.0 |
| 20 | 71.0 | 69.9 | 60.2 | 28.2 |
| 30 | 76.0 | 69.9 | 65.0 | 27.0 |
| 40 | 78.0 | 68.0 | 66.0 | 25.0 |
| 50 | 79.0 | 66.0 | 67.0 | 27.0 |
| 60 | 80.9 | 65.0 | 68.0 | 30.0 |
| 70 | 86.0 | 64.0 | 50.0 | 33.0 |
| 80 | 89.1 | 63.0 | 60.9 | 32.9 |
| 90 | 88.9 | 62.0 | 70.0 | 34.0 |
| 100 | 86.9 | 61.0 | 68.0 | 29.0 |

### 4.5 Throughput Ratio (%)

For fuzzy -enabled power industry systems, this article suggests profit maximization by incorporating the cooperation in compute load choices and material allocation. This paper presents a collaborative computing downloading framework for fuzzy-enabled MEC systems that work with a trusted model to simultaneously assess the cloud computing rate and fuzzy throughput. The research addresses the choice to load off, power allocation, block size, and interval to boost the weighted average cloud computing rate and transaction throughput of the fuzzy clustering system. Big data can improve the integrity of most immediate cloud transactions while increasing throughput and reducing latency thanks to its division into several subgroups. This article focuses on cloud computing and fuzzy challenges in throughput during instantaneous transactions. With a multi-target technique, the edge cloud computing system calculation rate and fuzzy system transaction throughput

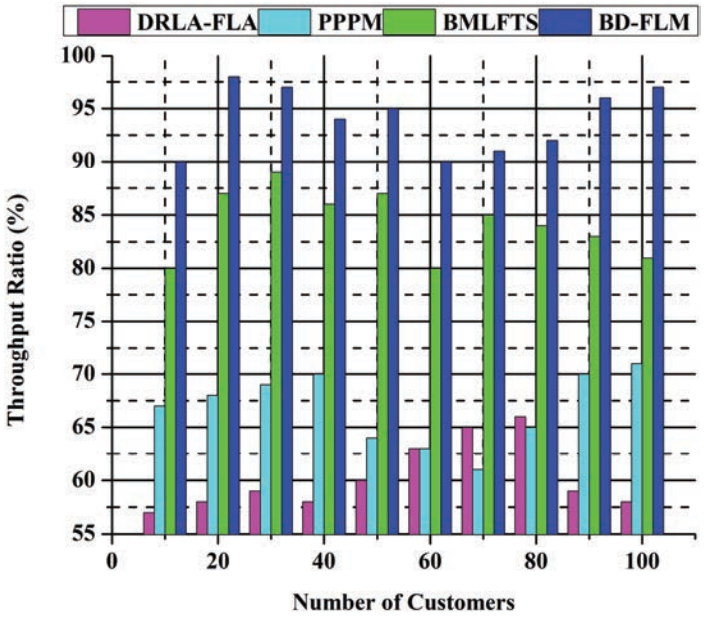


**Figure 8** Throughput ratio (%).

may both be improved. To enhance the performance of software-defined Industrial IoT systems, the trust characteristics and processing capacity of fuzzy clustering nodes and controllers were developed. Innovative, power industrial edge computing optimizes industrial IoT system performance and provides decentralization, latency, and system security for high-throughput requirements. Figure 8 shows the throughput ratio (%).

### 4.6 Data Transmission Rate (%)

Data transmission security may be improved by increasing cloud usage and accessibility efficiency by using communication security as one of the approaches. Cloud computing and internet consumer networks exchange data. A secure channel is needed to send data. When data is sent in plain text, it leaves the client and the server vulnerable. Identity and sensitive information may be stolen through the man-in-the-centre and fraud attacks by hackers. It's possible to use well-known authentication methods. All data travels across the internet when sent between cloud clients and the network of cloud service providers in the cloud. There are several dangers to data transfer. A hacker who gains access to the network can listen in on anything

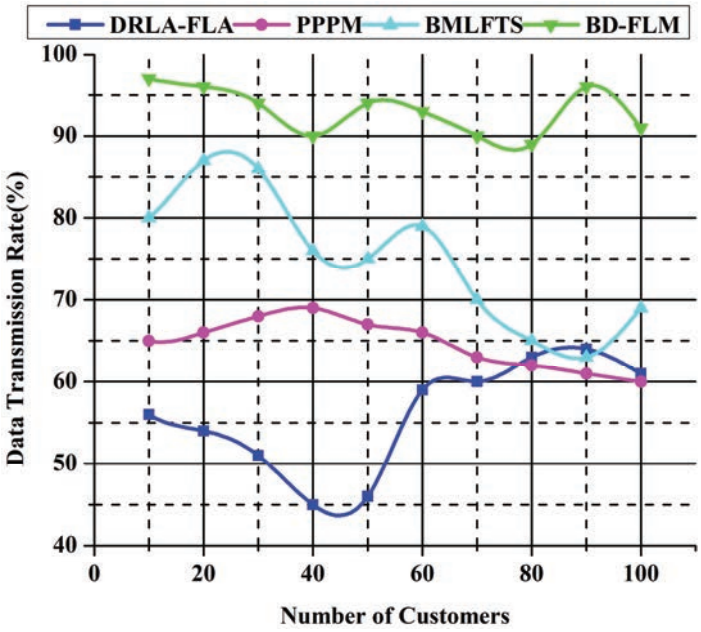


**Figure 9** Data transmission rate (%).

sent through it. Customer service suffers greatly when security procedures are not followed. Customers may rely on service providers to ensure their data is sent via a secure route. When transferring data, it must be encrypted. The usual fuzzy logic architecture is being extended by dispersing data processing and analysis over various communication protocols, a current trend in IoT. Many applications don't need raw data to be preserved, and just the analytic output is kept. As a result, sending data to the cloud in real-time is no longer the best strategy. It's critical to have a strong security policy since it entails distinct ownership and control when outsourcing data. Finally, even if no encryption is used during the transfer, the data layer can guarantee data transmission security. Figure 9 shows the data transmission rate (%).

## 5 Conclusion

Many electric utilities are hesitant about using large amounts of data from big data. In the future, energy management will need massive amounts of data to operate smart grids. Several roadblocks are standing in the way of smart grid big data applications' success. Big data integration with the smart grid has

just a limited amount of expertise at the moment. Businesses must concentrate on converting the data they acquire towards business intelligence to better serve customers and enhance procedures. This study suggests using Big Data-based fuzzy logic to preserve private information. The large data clustering-based privacy preservation probability model BD-FLM offers to create the least disturbance while keeping the most privacy. As a result, in a low carbon economy, solutions will be developed that increase efficiency and allow new methods to handle different parts of the utility to promote firm success and avoid risks from new rules and political involvement. The simulation results show that the suggested method beats the comparison algorithm for accuracy in making predictions. Individual privacy is protected while data accuracy improves due to predicting correct values. These extensive paper simulations show this proposed BD-FLM mechanism to achieve a security ratio of 98.5%, throughput ratio of 98.3%, data transmission rate of 97.4%, scalability rate of 97.2%, attack ratio of 98.0%, and low energy consumption rate of 25.0% when compared to other existing methods.

## References

[1] Amudha, G., and Narayanasamy, P. (2018). Distributed location and trust based replica detection in wireless sensor networks. Wireless Personal Communications, 102(4), 3303–3321.

[2] Gheisari, M., Najafabadi, H. E., Alzubi, J. A., Gao, J., Wang, G., Abbasi, A. A., and Castiglione, A. (2021). OBPP: An ontology-based framework for privacy-preserving in IoT-based smart city. Future Generation Computer Systems, 123, 1–13.

[3] Krishnamoorthy, S., Shanthini, A., Manogaran, G., Saravanan, V., Manickam, A., and Samuel, R. D. J. (2021). Regression Model-based Feature Filtering for Improving Hemorrhage Detection Accuracy in Diabetic Retinopathy Treatment. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 29(Supp01), 51–71.

[4] Manogaran, G., Shakeel, P. M., Baskar, S., Hsu, C. H., Kadry, S. N., Sundarasekar, R., ... and Muthu, B. A. (2020). FDM: Fuzzy-optimized data management technique for improving big data analytics. IEEE Transactions on Fuzzy Systems, 29(1), 177–185.

[5] Saravanan, V., Nuneviller, M., Pillai, A. S., and Anpalagan, A. (2020). Foundation of Big Data and Internet of Things: Applications and Case Study. Securing IoT and Big Data, 1–14.

[6] Amudha, G., Jayasri, T., Saipriya, K., Shivani, A., and Praneetha, C. H. Behavioural Based Online Comment Spammers in Social Media.

[7] Gao, J., Wang, H., and Shen, H. (2020). Task failure prediction in cloud data centers using deep learning. IEEE Transactions on Services Computing.

[8] Do, D. T., Van Nguyen, M. S., Nguyen, T. N., Li, X., and Choi, K. (2020). Enabling multiple power beacons for uplink of noma-enabled mobile edge computing in wirelessly powered IOT. IEEE Access, 8, 148892–148905.

[9] Seyhan, K., Nguyen, T. N., Akleylek, S., Cengiz, K., and Islam, S. H. (2021). Bi-GISISKE: Modified key exchange protocol with reusable keys for IoT security. Journal of Information Security and Applications, 58, 102788.

[10] Krishnamoorthy, S., Shanthini, A., Manogaran, G., Saravanan, V., Manickam, A., and Samuel, R. D. J. (2021). Regression Model-based Feature Filtering for Improving Hemorrhage Detection Accuracy in Diabetic Retinopathy Treatment. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 29(Supp01), 51–71.

[11] Manogaran, G., Baskar, S., Hsu, C. H., Kadry, S. N., Sundarasekar, R., Kumar, P. M., and Muthu, B. A. (2020). FDM: Fuzzy-optimized Data Management Technique for Improving Big Data Analytics. IEEE Transactions on Fuzzy Systems.

[12] Baskar, S., Shakeel, P. M., Sridhar, K. P., and Kanimozhi, R. (2019, July). Classification System for Lung Cancer Nodule Using Machine Learning Technique and CT Images. In 2019 International Conference on Communication and Electronics Systems (ICCES) (pp. 1957–1962). IEEE.

[13] Krishnan, E., Mohammed, R., Alnoor, A., Albahri, O. S., Zaidan, A. A., Alsattar, H., . . . and Alazab, M. (2021). Interval type 2 trapezoidal-fuzzy weighted with zero inconsistency combined with VIKOR for evaluating smart e-tourism applications. International Journal of Intelligent Systems.

[14] Sedik, A., Hammad, M., Abd El-Latif, A. A., El-Banby, G. M., Khalaf, A. A., Abd El-Samie, F. E., and Iliyasu, A. M. (2021). Deep Learning Modalities for Biometric Alteration Detection in 5G Networks-Based Secure Smart Cities. IEEE Access, 9, 94780–94788.

[15] Zhang, R., and Jackson Samuel, R. D. (2020). Fuzzy efficient energy smart home management system for renewable energy resources. Sustainability, 12(8), 3115.

[16] Sweeney, L. (2002). Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(05), 571–588.

[17] Diamantoulakis, P. D., Kapinas, V. M., and Karagiannidis, G. K. (2015). Big data analytics for dynamic energy management in smart grids. *Big Data Research*, *2*(3), 94–101.

[18] Zhang, Y., Huang, T., and Bompard, E. F. (2018). Big data analytics in smart grids: a review. *Energy informatics*, *1*(1), 1–24.

[19] Zhou, K., Fu, C., and Yang, S. (2016). Big data driven smart energy management: From big data to big insights. *Renewable and Sustainable Energy Reviews*, *56*, 215–225.

[20] Tannahill, B. K., and Jamshidi, M. (2014). System of Systems and Big Data analytics–Bridging the gap. *Computers & Electrical Engineering*, *40*(1), 2–15.

[21] Ren, Y., Leng, Y., Zhu, F., Wang, J., and Kim, H. J. (2019). Data storage mechanism based on blockchain with privacy protection in wireless body area network. *Sensors*, *19*(10), 2395.

[22] Tu, C., He, X., Shuai, Z., and Jiang, F. (2017). Big data issues in smart grid–A review. *Renewable and Sustainable Energy Reviews*, *79*, 1099–1107.

[23] Li, Y., Gai, K., Qiu, L., Qiu, M., and Zhao, H. (2017). Intelligent cryptography approach for secure distributed big data storage in cloud computing. *Information Sciences*, *387*, 103–115.

[24] Iqbal, S., Zhang, C., Arif, M., Hassan, M., and Ahmad, S. (2020). A new fuzzy time series forecasting method based on clustering and weighted average approach. *Journal of Intelligent & Fuzzy Systems*, *38*(5), 6089–6098.

[25] Alahakoon, D., and Yu, X. (2015). Smart electricity meter data intelligence for future energy systems: A survey. *IEEE Transactions on Industrial Informatics*, *12*(1), 425-436.

[26] Guo, Y., Zhao, Z., He, K., Lai, S., Xia, J., and Fan, L. (2021). Efficient and flexible management for industrial Internet of Things: A federated learning approach. *Computer Networks*, *192*, 108122.

[27] Batista, E., and Solanas, A. (2021). A uniformization-based approach to preserve individuals' privacy during process mining analyses. *Peer-to-Peer Networking and Applications*, *14*(3), 1500–1519.

[28] Shahbazi, Z., and Byun, Y. C. (2021). A Procedure for Tracing Supply Chains for Perishable Food Based on Blockchain, Machine Learning and Fuzzy Logic. *Electronics*, *10*(1), 41.

[29] Iqbal, R., Doctor, F., More, B., Mahmud, S., and Yousuf, U. (2020). Big data analytics: Computational intelligence techniques and application areas. *Technological Forecasting and Social Change*, *153*, 119253.
[30] Wang, H., Xu, Z., and Pedrycz, W. (2017). An overview on the roles of fuzzy set techniques in big data processing: Trends, challenges and opportunities. *Knowledge-Based Systems*, *118*, 15–30.
[31] Manogaran, G., Rawal, B. S., Saravanan, V., Kumar, P. M., Martínez, O. S., Crespo, R. G., . . . and Krishnamoorthy, S. (2020). Blockchain based integrated security measure for reliable service delegation in 6G communication environment. Computer Communications, 161, 248–256.
[32] Saravanan, V., Hussain, F., and Kshirasagar, N. (2022). Role of big data in Internet of Things networks. In Research Anthology on Big Data Analytics, Architectures, and Applications (pp. 336–363). IGI Global.
[33] Baskar, S., Shakeel, P. M., Kumar, R., Burhanuddin, M. A., and Sampath, R. (2020). A dynamic and interoperable communication framework for controlling the operations of wearable sensors in smart healthcare applications. Computer Communications, 149, 17–26.

## Biographies

**Feilu Hang** was born in 1984 in Zhaotong, Yunnan province, China. Graduated from Yunnan University with a master's degree in system Analysis and integration. At present, I am working in equipment management Department of information center of Yunnan Power Grid Co., LTD. His research interest covers network and information security.

**Linjiang Xie** was born in 1985 in Qujing, Yunnan Province, China. Graduated from Yunnan University with a bachelor's degree in information security. At present, I am working in equipment management Department of information center of Yunnan Power Grid Co., LTD. His research interest is network security operation.

**Zhenhong Zhang**, born in Qujing city, Yunnan Province, China in 1989, graduated from Beijing University of Posts and Telecommunications with a master's degree in computer technology. Currently, he is working in the equipment management department of information Center of Yunnan Power Grid Co., LTD., and his research direction is information system operation and maintenance.

**Wei Guo**, born in 1986 in Kunming, Yunnan Province, China, graduated from Chongqing University of Posts and Telecommunications with a bachelor's degree in Information Management and Information System. Currently, he is working in the equipment management department of information Center of Yunnan Power Grid Co., LTD. His research direction is network and network security operation and peacekeeping management.

**Hanruo Li** born in 1991 in Zhaotong, Yunnan, China, graduated from Fuzhou University with a bachelor's degree in network engineering. Currently, he is working in the equipment management Department of the information Center of Yunnan Power Grid Co., LTD. His research direction is network security operation and maintenance.