ZKG INTERNATIONAL

ISSN: 2366-1313

# PRIVACY PRESERVING DATA AGGREGATION FOR FOG BASED SMART GRIDS

**[1]D. KAVITHA, [2]A. UMAMAHESHWARI, [3]CH. NARESH KUMAR, [4]K. VARUN KUMAR**

[1]Assistant Professor, Dept.of IT, TKR College of Engineering & Technology, Meerpet, Hyderabad, davidikavitha2011@gmail.com

[2]BTech student, Dept.of IT, TKR College of Engineering & Technology, Meerpet, Hyderabad, umamaheshwariadlolu3910@gamil.com

[3]BTech student, Dept.of IT, TKR College of Engineering & Technology, Meerpet, Hyderabad, cnareshkumar.1719@gmail.com

[4]BTech student, Dept.of IT, TKR College of Engineering & Technology, Meerpet, Hyderabad, kongarivarunk@gmail.com

***Abstract***: *The increasingly powerful and extensive deployment of edge devices, edge/fog computing enables customers to manage and analyses data locally, and extends computing power and data analysis applications to network edges. Meanwhile, as the next generation of the power grid, the smart grid can achieve the goal of efficiency, economy, security, reliability, use safety and environmental friendliness for the power grid. However, privacy and secure issues in fog-based smart grid communications are challenging. Without proper protection, customers' privacy will be readily violated. This paper presents a smart and practical Privacy-preserving Data Aggregation (PDA) scheme with smart pricing and packing method for fog-based smart grids, which achieves diversified tariffs, multifunctional statistics and efficiency. Especially, we first propose a smart PDA scheme with Smart Pricing (PDA-SP). With PDA-SP, the Control Center (CC) can compute more complex and higher-order aggregation statistics to provide various services, provide diversiform pricing strategies and choose a double-winning strategy. Subsequently, we put forward a practical PDA scheme with Packing Method (PDA-PM), which is able to reduce the size of encrypted data and improve performance in performing various secure computations. Moreover, we extend our original packing method and present a more useful packing method, which can handle general vectors with large entries. The security analysis shows that our proposed scheme is secure against many threats. The performance evaluation reveals that the computation and communication overheads of our proposed scheme are effectively reduced*

ISSN: 2366-1313

*by employing the Somewhat Homomorphic Encryption (SHE), and our packing method can further significantly reduce these overheads.*

***Keywords:*** *Somewhat Homomorphic Encryption, Privacy-preserving Data Aggregation, Somewhat Homomorphic Encryption.*

## I. INTRODUCTION

Fog/Edge computing extends from cloud computing and has boomed in recent years. It enables customers to perform computing, connectivity, and storage locally, and extends cloud computing capabilities to the fringes of society. In big data technology, users have higher expectations for exceptional service and overall network performance. Traditional cloud computing suffers from a general lack of garage capabilities and computing power, even to handle a wide variety of customer inquiries and feedback. Therefore, it is very useful to transfer some cloud functions to the fog node. Fog/area computing has the advantages of fast reaction, low delay, fog variability, massive site belief, superior security and reliability in evaluation using cloud computing. The aforementioned remarkable benefits have contributed to the emergence of fully intelligent networks based on fog and other Industrial Internet of Things [1].

As the upcoming power grid era, the smart grid can achieve the goal of performance, economic system, safety and reliability, use protection and environmental friendliness of the power grid. The fog node allows the application owner to provide various services through service query and command control between clients and the CC, including energy price adjustment, total energy consumption gain, energy charging for the user and additional energy provision according to customer needs.

However, it is very difficult for privacy and security in fog-based smart network connections. Since electricity usage statistics include customers' energy usage patterns, which may be closely related to their private lives, mishandling of these records may also expose customer privacy [2].

In addition, diversified price lists, multi-function and efficiency data should also be considered with caution. First, traditional tariffs often use fixed prices to calculate energy payments to customers and consider restrictive pricing techniques. With the improvement of smart grids and fog-based power grids, these traditional

ISSN: 2366-1313

price lists are insufficient to meet the needs of honest pricing and smart digital devices. Therefore, it is necessary to propose a diverse PDA scheme (which can gain different rates). Secondly, with the increasing demands of energy consumers, in order to provide many services, CC needs to calculate more complex and better-order statistical capabilities. However, many of the previous works are only useful for symmetric multiplication of a single intensity, which is not efficient enough. Therefore, it is of great interest to propose a multifunctional PDA scheme (supports CC to calculate statistical functions whose degree is greater than 2). Third, CC, fog nodes, and clients have to spend as little as possible on computing and communications. However, the binary coupling technique is used in many older works, which puts a heavy burden on CC and fog nodes. It is necessary to provide an effective PDA scheme for fog-based smart grids [3].

To achieve different definitions, multifunctional data, and performance, in this paper, we recommend a reasonable smart PDA scheme for fully intelligent fog-based networks with smart pricing and packaging technology. We conclude our contributions as follows. Almost all of the previous work only considers fixed prices or alternative pricing strategies are restricted, and traditional prices are insufficient to meet the fair pricing requirements. In response to such desires, we introduce smart pricing in the smart grid primarily based on fog. With its normal functions, CC can offer various pricing strategies and indirectly guide customers to dynamically adjust their electricity usage patterns, mainly based on changes in energy prices. In addition, our proposed scheme can also perform a one-way evaluation of variance (ANOVA) to assess whether these pricing strategies have an effect on energy use behaviour of customers and to choose a win-win method.

• Because CC may also need to calculate higher-order and more complex statistical capabilities to provide various representations, we introduce a multifunctional PDA scheme, which is not only more effective for multifunctional additive and non-additive groupings, but also helps CC calculate statistical functions whose level is larger from 2. In addition, we also introduce two kinds of fog-based fully intelligent network minimum aggregation protocols, and compare the computation overhead and verbal exchange between them.

ISSN: 2366-1313

• To reduce the size of encrypted data and improve performance while performing multiple secure computations, we created a new encapsulation method for

Our PDA schemes. Our new packing technique provides 4 types of vectors packed ciphertext, which differs from the message encoding method provided by Lauter, Naehrig, and Vaikuntanathan [4], and makes our proposed scheme as efficient in both ciphertext length as in overall performance. In addition, we introduce a more useful encapsulation method that can handle generic vectors with large inputs.

**PURPOSE**

1. The increasingly powerful and extensive deployment of edge devices, edge/fog computing enables customers to manage and analyses data locally, and extends computing power and data analysis applications to network edges. Our scheme is to achieve multifunctional and efficient PDA.

2.Statistic-oriented PDA which is designed to perform various statistical analyses on remote sensing data, and efficiency-oriented PDA which focuses on raising efficiency.

This is to achieve multifunctional and efficient PDA, which is similar to a lot of related works published in recent literatures. Generally, there are two groups of PDA schemes: statistic-oriented PDA which is designed to perform various statistical analyses on remote sensing data, and efficiency-oriented PDA which focuses on raising efficiency.

## II. LITERATURE SURVEY

In [5] In the Internet of Things (IoT), aggregation and release of real-time data can often be used for mining more useful information so as to make humans lives more convenient and efficient. However, privacy disclosure is one of the most concerning issues because sensitive information usually comes with users in aggregated data. Thus, various data encryption technologies have emerged to achieve privacy preserving. These technologies may not only introduce complicated computing and high communication overhead but also do not work on the protection of endless data streams. Considering these challenges, we propose a real-time stream data aggregation framework with adaptive ω-event differential privacy (Re-ADP). Based on adaptive ω-event differential privacy, the framework can protect any data collected by sensors over any dynamic ω time stamp successively over infinite stream.

ISSN: 2366-1313

It is designed for the fog computing architecture that dramatically extends the cloud computing to the edge of networks. In our proposed framework, fog servers will only send aggregated secure data to cloud servers, which can relieve the computing overhead of cloud servers, improve communication efficiency, and protect data privacy.

Finally, experimental results demonstrate that our framework outperforms the existing methods and improves data availability with stronger privacy.

In [6] Internet of Things (IoT) is gaining increasing popularity. Overwhelming volumes of data are generated by IoT devices. Those data after analytics provide significant information that could greatly benefit IoT applications. Different from traditional applications, IoT applications, such as environmental monitoring, smart navigation, and smart healthcare come with new requirements, such as mobility, real-time response, and location awareness. However, traditional cloud computing paradigm cannot satisfy these demands due to centralized processing and being far away from local devices. Hence, edge computing was introduced to perform data processing and storage in the edge of networks, which is closer to data sources than cloud computing, thus efficient and location-aware. Unfortunately, edge computing brings new security and privacy challenges when applied to data analytics.

The literature still lacks a thorough review on the recent advances in secure data analytics in edge computing. In this paper, we first introduce the concept and features of edge computing, and then propose a number of requirements for its secure data analytics by analyzing potential security threats in edge computing. Furthermore, we give a comprehensive review on the pros and cons of the existing works on data analytics in edge computing based on our proposed requirement.

In [7] IoT is envisioned as the next stage of the information revolution, enabling various daily applications and providing better service by conducting a deep fusion with cloud and fog computing. As the key mission of most IoT applications, data management, especially the fundamental function-data query, has long been plagued by severe security and privacy problems. Most query service providers, including the big ones (e.g., Google, Facebook, Amazon, and so on) are suffering from intensive attacks launched by insiders or outsiders. As a consequence, processing various queries in IoT without compromising the data and query privacy is an urgent and challenging issue. In this

ISSN: 2366-1313

article, we propose a thing-fog-cloud architecture for secure query processing based on wellstudied classical paradigms. Following with a description of crucial technical challenges in terms of functionality, privacy and efficiency assurance, we survey the latest milestone-like approaches, and provide an insight into the advantages and limitations of each scheme. Based on the recent advances, we also discuss future research opportunities to motivate efforts to develop practical private query protocols in IoT.

In [8] Data aggregation plays an important role in the Internet of Things, and its study and analysis has resulted in a range of innovative services and benefits for people. However, the privacy issues associated with raw sensory data raise significant concerns due to the sensitive nature of the user information it often contains. Thus, numerous schemes have been proposed over the last few decades to preserve the privacy of users' data. Most methods are based on encryption technology, which is computationally and communicationally expensive. In addition, most methods can only handle a single aggregation function. Therefore, in this paper, we propose a multifunctional data aggregation method with differential privacy. The method is based on machine learning and can support a wide range of statistical aggregation functions, including additive and non-additive aggregation. It operates within a fog computing architecture, which extends cloud computing to the edge of the network, alleviating much of the computational burden on the cloud server. And, by only reporting the results of the aggregation to the server, communication efficiency is improved. Extensive experimental results show that the proposed method not only answers flexible aggregation queries that meet diversified aggregation goals, but also produces aggregation results with high accuracy.

In [9] Smart grid enables two-way communications between smart meters and operation centers to collect real-time power consumption of customers to improve flexibility, reliability, and efficiency of the power system. It brings serious privacy issues to customers, since the meter readings possibly expose customers' activities in the house. Data encryption can protect the readings, but lengthens the data size. Secure data aggregation improves communication efficiency and preserves customers' privacy, while fails to support dynamic billing, or offer integrity protection against public collectors, which may be hacked in reality. In this paper, we define a new

ISSN: 2366-1313

security model to formalize the misbehavior of collectors, in which the misbehaving collectors may launch pollution attacks to corrupt power consumption data.

## III. PROPOSED METHODOLOGY

For achieving diversified tariffs, multifunctional statistics and efficiency, in this paper, we propose a smart and practical PDA scheme for fog-based smart grids with smart pricing and packing method. We conclude our contributions as follows:

• Almost all the previous works are only taking fixed pricing into consideration or the alternative pricing strategies are limited, and traditional tariffs are insufficient to meet the requirements of fair pricing. In response to such needs, we introduce smart pricing into the fog-based smart grid. Thanks to its peculiar features, the CC can provide diversiform pricing strategies, and indirectly guide customers to dynamically adjust their energy usage patterns based on changes in electricity prices. In addition, our proposed scheme also can perform one-way analysis of variance (ANOVA) to evaluate whether these pricing strategies have an impact on customers' electricity usage behavior, and choose a double-winning strategy.

• As the CC may need to compute more complex and higher-order statistic functions to provide various services, we introduce a multifunctional PDA scheme, which not only supports multifunctional additive and non-additive aggregations, but also supports the CC to calculate statistic functions whose degree is larger than 2. In addition, we also present two types of min aggregation protocols for fog-based smart grids, and compare the computation and communication overheads of them.

• For reducing the size of encrypted data and improving performance when performing various secure computations, we come up with a new packing

method for our PDA scheme. Our new packing method provides four types of packed ciphertexts for vectors, which is different from the message encoding technique presented by Lauter, Naehrig and Vaikuntanathan, and makes our proposed scheme efficient in both ciphertext size and performance. In addition, we present a more useful packing method, which can handle general vectors with large entries.

• We introduce SHE into the fog-based smart grid, compared with previous works that utilizing bilinear pairing and

ISSN: 2366-1313

homomorphic encryption, the computation and communication overheads are effectively reduced. Furthermore, the performance evaluation reveals that our packing method can further significantly reduce these overheads, which means our scheme is lightweight and efficient.

## SYSTEM ARCHITECTURE

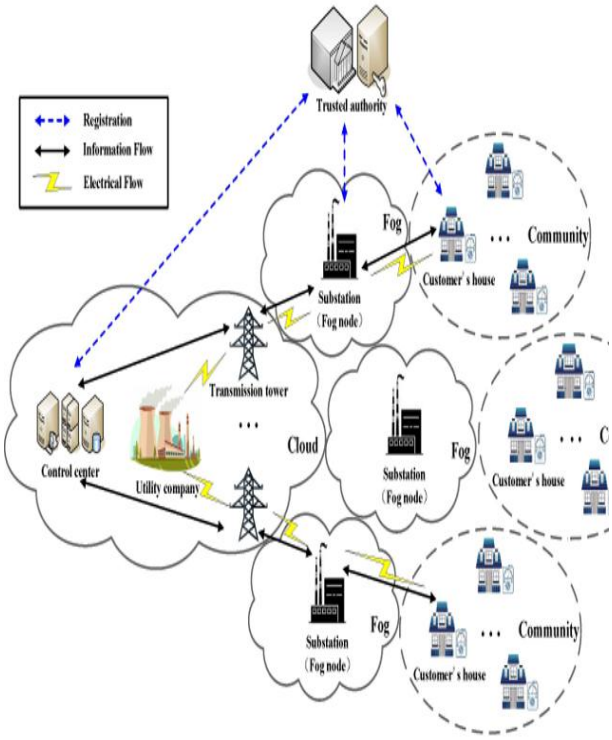


Fig.1 System architecture

### System Model

The fog-based smart grid system consists of a trusted authority (TA), a utility company and a CC, some substations and some fog nodes, some communities and each community contains a number of customers, which are equipped with smart meters. Figure 1 describes our system model.

• **Trusted Authority**: The TA takes charge of entity registration and it is a powerful third party. It will go off-line after booting the whole system.

• **Control Center and Utility Company**: The CC collects, processes and analyzes real-time smart meter data and issues grid commands to smart meters and substations to provide customers with reliable grid services. The utility company is responsible for electrical power generation, storage and distribution.

• **Fog Node and Substation:** The flows of information between customers' smart meters and the CC, which contain smart meter readings, requests and commands, are preserved, processed and forwarded by the fog node. The substation waits for the utility company's commands and stores the electricity and transmits the electricity power to customers' houses.

• **Customer**: Each customer's house with a smart meter, which gathers electricity usage data in real-time, relays these data and requests of grid service to the CC.

### File encryption

The principal module in this venture is record encryption module. This module is

ISSN: 2366-1313

intended for scramble the document prior to re-appropriating the record into cloud specialist organizations. The encryption cycle done by the unique information proprietor to keep their information from the unapproved clients. During the encryption time the mysterious key for the record to unscramble the document is created. The proprietors need to maintain the mystery key. At the point when they are recovering the information from the cloud specialist organizations the information will be in encoded structure. So, this module assumes a significant part in our venture.

**File decryption**

The last module in this venture is record unscrambling. In this module the scrambled record will return once more into its unique structure. For the decoding interaction the calculation need the key which made at the hour of encryption. The information proprietor keeps the key created at encryption measure. After enter the key the calculation will decode the document and returns the information in a lucid way which can be perceived by the clients.

**Design Goal**

Our design goal is to present a multifunctional, diversiform and efficient PDA scheme for fog-based smart grids. Specifically, we should realize the following three goals.

• The proposed scheme should guarantee diversified tariffs. For meeting the requirements of fair pricing and providing diversiform pricing strategies, the proposed scheme should guarantee diversified tariffs, so that the CC can guide customers to dynamically adjust their energy usage patterns based on changes in electricity prices.

• The proposed scheme should support multifunctional statistics. Although many previous works have realized multifunctional addition and non-addition aggregations, these works are only supporting one-depth homomorphic multiplication. With the ever-increasing demands from power consumers, the proposed scheme should support the CC to aggregate the customer's electricity usage data in a privacy-preserving way for any given statistic function whose degree is larger than 2. By this way, the CC can compute more complex and higher-order statistic functions to provide various services. Specially, the proposed scheme should support diversiform statistical functions of customers' electricity usage data, such as sum, inner product, one-way ANOVA, max and min.

ISSN: 2366-1313

• The proposed scheme should achieve efficiency. Although a lot of previous works have employed bilinear pairing and homomorphic encryption to realize efficient PDA, these works involve bilinear pairing operations and pose a heavy burden on the CC and fog nodes. Thus, the proposed scheme should achieve PDA in an efficient way.

## IV. RESULTS

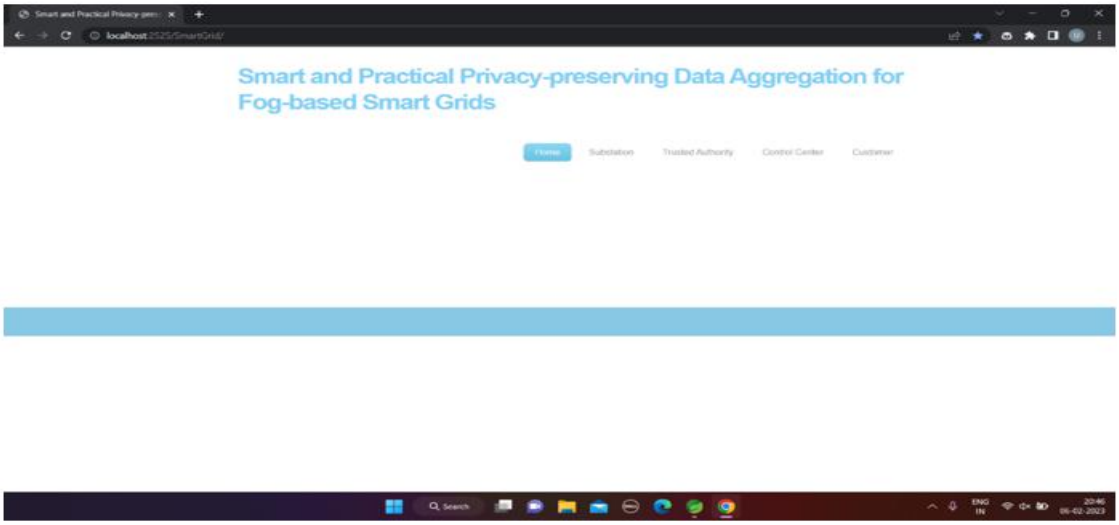


Fig.2 Login page

Customer login page to register customer details

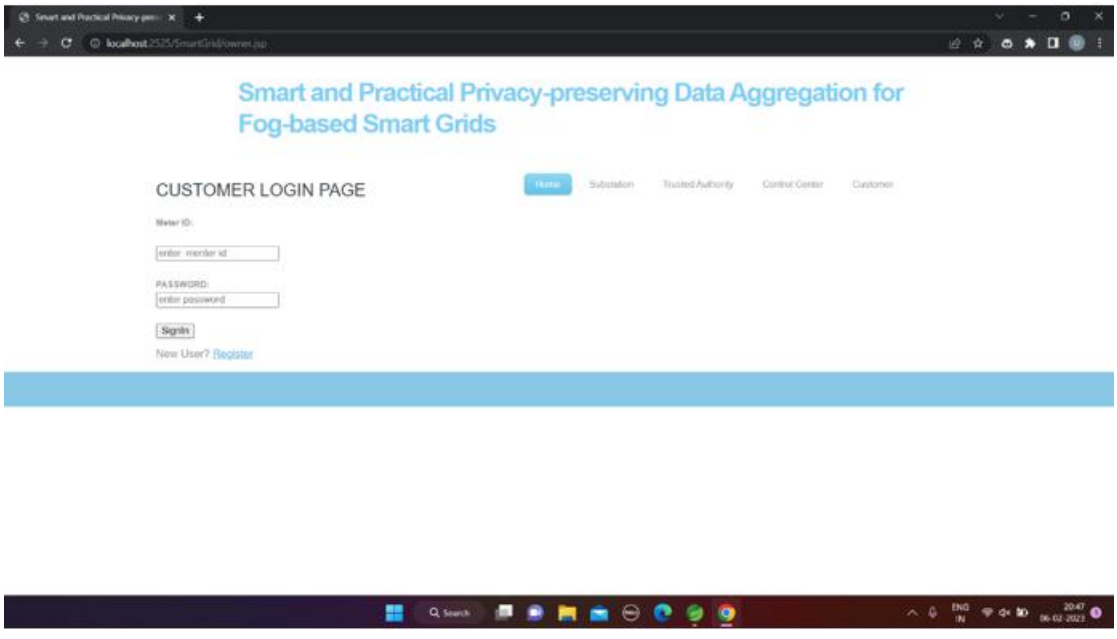


Fig.3 Customer login page

ISSN: 2366-1313

After adding customer details the bill is uploaded to the cloud

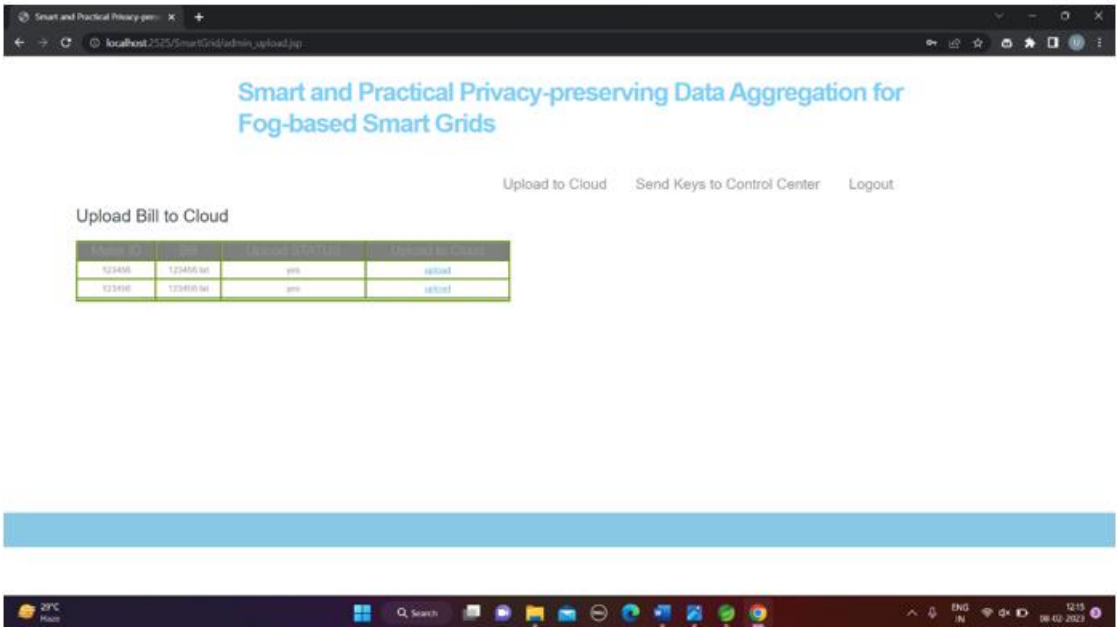


Fig. 4 Uploading bill to cloud

Cloud drive saves the Customer details in the form of Encrypted format Bill at smart grid

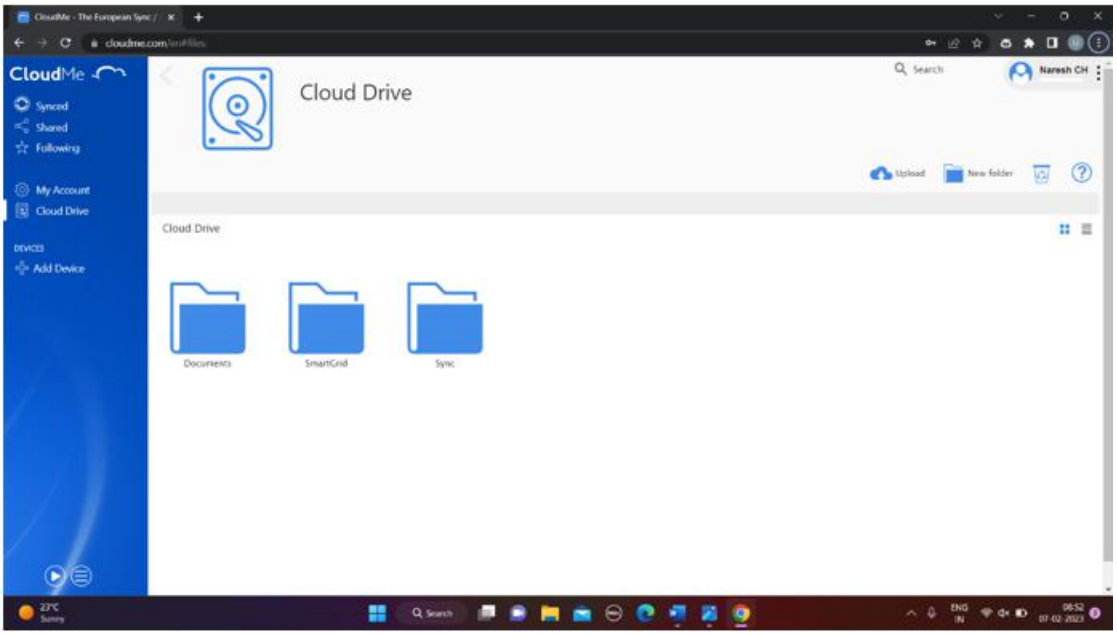


Fig.5 Cloud Drive

ISSN: 2366-1313

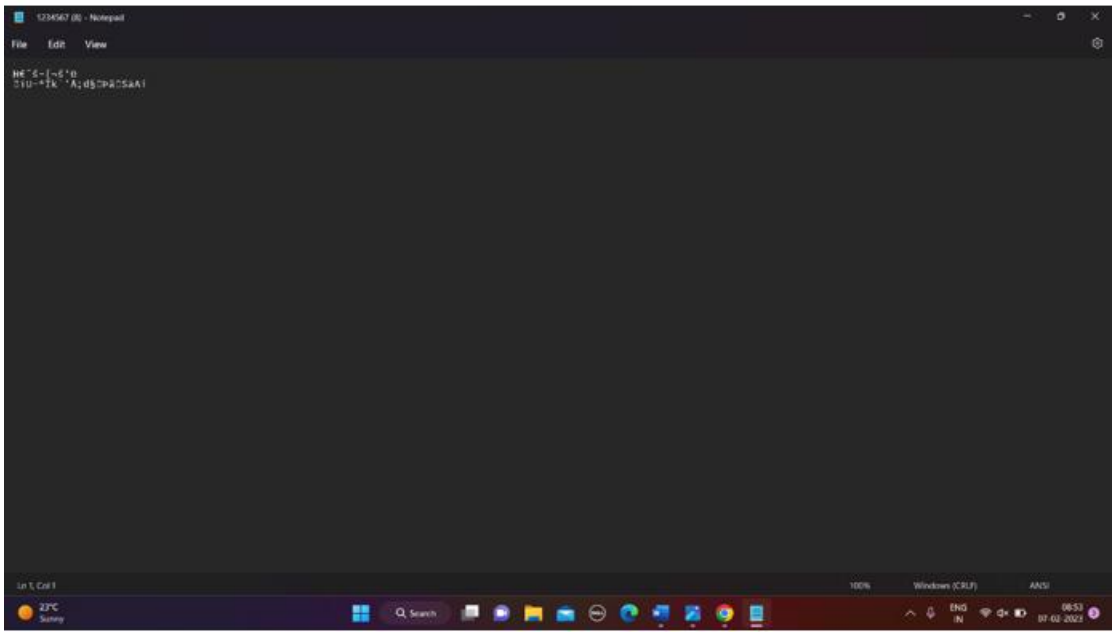

Fig. 6 Encrypted format bill

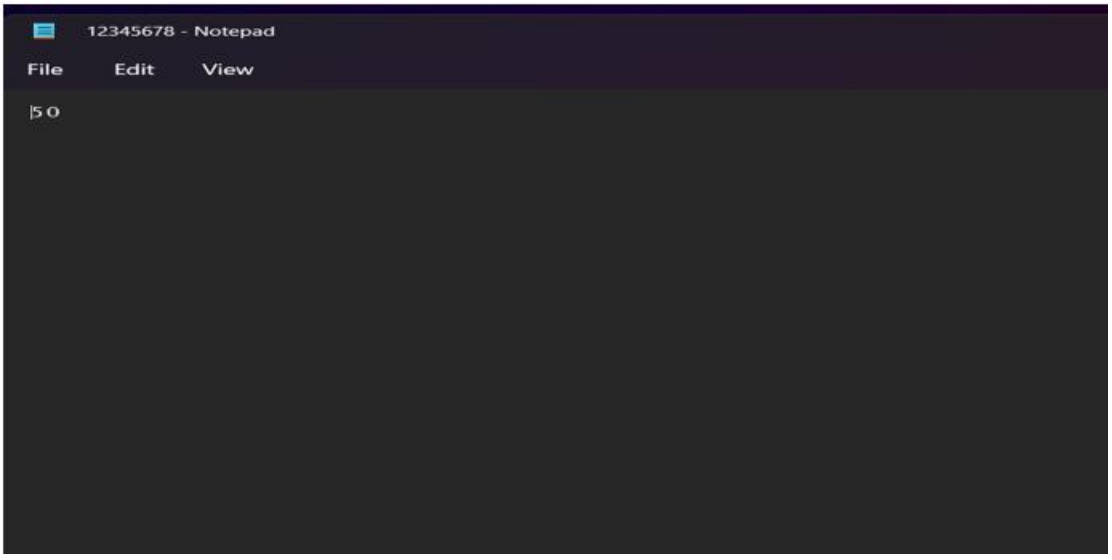


Fig.7 Decrypted format bill

The above fig shows that encrypted bill is converted into decrypted format and cutomer can be view their bill&pay.

## V. CONCLUSION

we have proposed a smart and practical PDA scheme with smart pricing and packing method for fog based smart grids, which achieved multifunctional statistics diversified tariffs and efficiency. At first, we have presented a scheme named PDA-SP. With PDA-SP, the CC could provide

ISSN: 2366-1313

diversiform pricing strategies, choose a double-winning strategy, and compute more complex and higher-order statistic functions to provide various services. Second, we have presented a scheme named PDA-PM, which could reduce the size of encrypted data and improve performance in performing various secure computations. Moreover, the improved version also could handle general vectors with large entries. At last, the security analysis showed that our proposed scheme was secure against many threats, and the performance evaluation revealed that our proposed scheme was lightweight and efficient.

## REFERENCES

[1] Y. Huo, C. Yong, and Y. Lu, "Re-adp: Real-time data aggregation with adaptive-event differential privacy for fog computing," Wireless Communications and Mobile Computing, vol. 2018, 2018.

[2] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," IEEE Internet of Things Journal, 2019.

[3] Prasadu Peddi. An efficient analysis of stocks data using mapreduce. ISSN: 1320, 682:22–34, 2019.

[4] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in internet of things with privacy preserving: Challenges, solutions and opportunities," IEEE Network, vol. 32, no. 6, pp. 144–151, 2018.

[5] M. Yang, T. Zhu, B. Liu, Y. Xiang, and W. Zhou, "Machine learning differential privacy with multifunctional aggregation in a fog computing architecture," IEEE Access, vol. 6, pp. 17 119–17 129, 2018.

[6] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Balancing security and efficiency for smart metering against misbehaving collectors," IEEE Transactions on Smart Grid, vol. 10, no. 2, pp. 1225–1236, 2017.

[7] S. Desai, R. Alhadad, N. Chilamkurti, and A. Mahmood, "A survey of privacy preserving schemes in ioe enabled smart grid advanced metering infrastructure," Cluster Computing, vol. 22, no. 1, pp. 43–69, 2019.

[8] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," IEEE Communications Magazine, vol. 56, no. 7, pp. 82–88, 2018.

[9] 8. Prasadu Peddi (2019), "Data Pull out andfacts unearthing in biological Databases", International Journal of

ISSN: 2366-1313

Techno-Engineering, Vol. 11, issue 1, pp: 25-32.

[9] R. Lu, Privacy-enhancing aggregation techniques for smart grid communications. Springer, 2016.