Notification of Acceptance of the AICCC 2023

Kyoto, 16-18 December, 2023

http://www.aiccc.net/

Paper ID: CA0055

Paper Title: Let's Hide from LLMs: An Adaptive Contextual Privacy Preservation Method for Time Series Data

Dear Ubaid Ur Rehman, Musarrat Hussain, Tri D.T. Nguyen and Sungyoung Lee,

First of all, thank you for your concern. 2023 6th Artificial Intelligence and Cloud Computing Conference (AICCC 2023) review procedure has been finished. Your paper was tripling blind-reviewed and, based on the evaluations. The comments are enclosed.

The selected papers could be published in the international conference proceeding with high quality. According to the recommendations from reviewers and technical program committees, we are glad to inform you that your paper identified above have been selected for publication and oral presentation. You are invited to present your paper and studies during our AICCC conference that would be held during December 16-18, 2023.

All peer reviewed and accepted papers can be published in the Conference Proceedings by ACM (ISBN: 979-8-4007-1622-5) and be indexed by Ei Compendex and Scopus, and submitted to be reviewed by Thomson Reuters Conference Proceedings Citation Index (ISI Web of Science).

(Important Steps for your registration): Please do finish all the 4 steps on time to guarantee the paper published in the proceedings successfully:

1. Revise your paper according to the Review Comments in the attachment carefully.

2. Format your paper according to the Formatting Instructions carefully.
http://www.aiccc.net/template.docx (DOC Format)

3. Register through the link directly:

https://www.zmeeting.org/register/aiccc2023

4. Add the CCS Concepts part and XML code in your paper.
http://www.aiccc.net/CCS&XML.docx

Note: To register through the link above, you are required to sign in the system first. Please do fill the registration information required, upload the final paper, payment proof in the system before November 27, 2023 to guarantee the registration successfully.

AICCC 2023 will check the format of all the registered papers and send e-mail confirmation to the authors. After the registration, we will send all qualified papers to the publish house and index organization for publishing directly.

We are looking forward to meeting all the authors in our conference.

Please strictly adhere to the format specified in the conference template while preparing your final paper. If you have any problem, please feel free to contact us via **aiccc.contact@gmail.com.** For the most updated information on the conference, please check the conference website at **http://www.aiccc.net/.** The Conference Program will be available at the website in **the early of December, 2023**.

Yours sincerely,

www.aiccc.net

AICCC 2023

AICCC&ADIP 2023

KYOTO CONFERENCE ABSTRACT

Kyoto, Japan
December 16-18, 2023

2023 6TH ARTIFICIAL INTELLIGENCE AND CLOUD COMPUTING CONFERENCE **AICCC**

2023 5TH ASIA DIGITAL IMAGE PROCESSING CONFERENCE **ADIP**

Registration and Zoom test (Online)

Online Zoom Test-December 16, 2023

Japan Local Time (GMT+9)

*Online test is for testing the Internet connection and helping participants get familiar with software Zoom, b
make sure that you will attend online test.

Zoom link: https://us02web.zoom.us/j/83229506745

Zoom Room ID: 83229506745

10:10-10:20	Keynote speaker	Prof. Wenbing Zhao
10:20-10:30	Keynote speaker	Prof. Yan Li
10:30-11:00	Session 6 (Online)	CA0036, CA0030, CA5004-A, CA5007-A, CA0029, CA5001
11:00-11:30	Session 7 (Online)	CA0053, CA0068, CA0080, CA0079
11:30-12:00	Session 8 (Online)	CA0031, CA0052, CA0059, CA2003, CA0034, CA0070
16:00-16:05	Invited Speaker	Prof. Narendra D. Londhe
16:05-16:10	Invited Speaker	Prof. Umesh C. Pati
16:10-16:15	Invited Speaker	Prof. Pascal Lorenz
16:15-16:20	Invited Speaker	Prof. Tossapon Boongoen

Schedule Simple Version

Tips: The time in the schedule is according to Japan Standard Time (GMT+9)

*Regular Oral Presentation: about **15 Minutes** including Presentation and **2-3 Minutes** for Question and Answer.

December 17, 2023- Keynote Speeches, Invited Speeches and Onsite Sessions

Japan Local Time (GMT+9)

Zoom link: https://us02web.zoom.us/j/83229506745

Zoom Room ID: 83229506745

Time	Each talk includes Q&A time	Presenter	Room
9:00-9:05	Opening Remark	Prof. Seiichi Ozawa, Kobe University, Japan	9F Shiho(紫峰) Zoom ID: 83229506745
9:05-9:45	Keynote Speech 1 Speech Title: Digital Economy Demands 5G/6G Networks, Generative AI, and Intelligent Twin City	Prof. Kai Hwang, The Chinese University of Hong Kong (Shenzhen), China (IEEE Life Fellow)	
9:45-10:25	Keynote Speech 2 Speech Title: Fine-Grained Activity Recognition in Professional Sports: A Preliminary Study	Prof. Wenbing Zhao, Cleveland State University, USA	
10:25-10:40	Group Photo & Coffee Break		
10:40-12:10	Session 1 Topic: Neural Network Models and Data Computing Session Chair: Prof. Dmitriy K. Levonevskiy, St. Petersburg Federal Research Center of the Russian Academy of Sciences, Russia	CA0050, CA0056-A, CA0060, CA0076-A, CA0027, CA0055	
12:10-13:00	Lunch Time		9F Hakusui(白水)
13:00-13:40	Keynote Speech 3 Speech Title: Small-data Deep Learning for AI-Aided Diagnosis and AI Medical Imaging	Prof. Kenji Suzuki, Tokyo Institute of Technology, Japan	9F Hakusui(白水) Zoom ID: 83229506745
13:40-14:20	Keynote Speech 4 Speech Title: Sleep Stages Classification Using Deep Learning Methods	Prof. Yan Li, University of Southern Queensland, Australia	

14:20-14:40	Invited Speech 1 Speech Title: Video-based Intrusion Detection System using Deep Learning Techniques	Prof. Umesh C. Pati, National Institute of Technology (NIT), India	
14:40-16:10	Parallel Session 2 Topic: Intelligent system monitoring and information management based on IoT Session Chair: Prof. Herlina Abdul Rahim, University of Technology Malaysia, Malaysia	CA0004, CA0021, CA0024, CA0032, CA0046, CA0047	9F Hakusui(
	Parallel Session 3 Topic: Next generation artificial intelligence technology and applications Session Chair: Prof. Ahmad Al-Qerem, Zarqa University, Jordan	CA0005-A, CA0010, CA0048, CA0057, CA2002, CA0049	9F Benihana(
16:10-16:25	Coffee Break		9F Hakusui 2:00-1 Benihana (白水+紅 3:30-
16:25-18:10	Parallel Session 4 Topic: Machine Learning and Prediction Models Session Chair: Assoc. Prof. Swee Chuan Tan, Singapore University of Social Sciences, Singapore	CA0002, CA0033-A, CA5016, CA0054, CA5011, CA0016, CA0082-A	9F Hakusui(白 3:50-
	Parallel Session 5 Topic: Intelligent Image Analysis and Processing Methods Session Chair: Prof. Kenji Suzuki, Tokyo Institute of Technology, Japan	CA0065-A, CA5014, CA5002-A, CA5010, CA5003-A, CA5013, CA5005-A, CA0058(Poster)	9F Benihana(紅 4:50 5:0
18:10-20:00	Dinner Time		9F Hakaku(八 5:2

December 18, 2023- Invited Speeches and Online Sessions

Japan Local Time (GMT+9)

Zoom link: https://us02web.zoom.us/j/83229506745

Zoom Room ID: 83229506745

Time	Each talk includes Q&A time	Presenter
10:50-12:00	Session 6 Topic: Image detection and speech recognition Session chair: Assoc. Prof. Ts. Dr Hamimah binti Ujir, Universiti Malaysia Sarawak, Malaysia	CA0036, CA0030, CA5004-A, CA5007-A, CA0029, CA5001
12:00-13:30	Lunch Time	
13:30-13:50	Invited Speech 2 Speech Title: Multiparametric Behavioral Machine Based Pain Estimation	Prof. Narendra D. Londhe, National Institute of Technology Raipur, India
13:50-14:50	Session 7 Topic: Information Privacy and Security in Data Networks Session chair: Prof. Anand Nayyar, Duy Tan University, Viet Nam	CA0053, CA0068, CA0080, CA0079
14:50-15:00	Break time	
15:00-15:20	Invited Speech 3 Speech Title: Advanced architectures of Next Generation Wireless Networks	Prof. Pascal Lorenz, University of Haute-Alsace, France
15:20-15:40	Invited Speech 4 Speech Title: Imperfect data, the curse for any data science project.	Prof. Tossapon Boongoen, Aberystwyth University, UK
15:40-17:10	Session 8 Topic: AI based data computing and recommendation system Session Chair:	CA0031, CA0052, CA0059, CA2003, CA0034, CA0070

computations, particularly

CA0055 (11:55-12:10 GMT+9)

Let's Hide from LLMs: An Adaptive Contextual Privacy Preservation Method for Time Series Data

Ubaid Ur Rehman, Musarrat Hussain, Tri D.T. Nguyen and Sungyoung Lee

Kyung Hee University, South Korea

Abstract-The emergence of the Internet of Things (IoT) has evolved various application areas, such as healthcare, smart energy management, and autonomous vehicles. These devices continuously transmit time-series data that can be utilized by a variety of applications to provide personalized services. Recently, Large Language Models (LLMs) have been widely adopted in these application areas to input time-series data into prompts for in-context learning and to retrieve relevant responses accordingly. The time-series data contains sensitive information, and its processing can lead to privacy concerns. Several solutions have been proposed in the literature using differential privacy, which protects single data points or batch-wise privacy preservation through manual configuration of the privacy parameter (ε). In this paper, we propose an adaptive contextual privacy preservation method that analyzes the data attributes required for specific application services, acting as context. It then identifies sensitive attributes and adaptively selects the value of ε for each data attribute to maintain a balance between privacy and service requirements. The proposed approach was evaluated using power consumption and solar power generation datasets. The results show that the proposed approach dynamically selects the privacy parameter for each data attribute. Moreover, the original and anonymized data were fed into the prompt to assess the textual responses generated by LLM. The results show that our proposed approach achieved an average degree of semantic similarity score of 94.5% for power consumption data and 95.23% for solar power generation data.

Let's Hide from LLMs: An Adaptive Contextual Privacy Preservation Method for Time Series Data

UBAID UR REHMAN

Kyung Hee University (Global Campus), Yongin-si, Republic of Korea.

ubaid.rehman@khu.ac.kr

MUSARRAT HUSSAIN

Kyung Hee University (Global Campus), Yongin-si, Republic of Korea.

Musarrat.hussain@oslab.khu.ac.kr

TRI D.T. NGUYEN

Kyung Hee University (Global Campus), Yongin-si, Republic of Korea.

tringuyendt@khu.ac.kr

SUNGYOUNG LEE

Kyung Hee University (Global Campus), Yongin-si, Republic of Korea.

sylee@oslab.khu.ac.kr

The emergence of the Internet of Things (IoT) has evolved various application areas, such as healthcare, smart energy management, and autonomous vehicles. These devices continuously transmit time-series data that can be utilized by a variety of applications to provide personalized services. Recently, Large Language Models (LLMs) have been widely adopted in these application areas to input time-series data into prompts for in-context learning and to retrieve relevant responses accordingly. The time-series data contains sensitive information, and its processing can lead to privacy concerns. Several solutions have been proposed in the literature using differential privacy, which protects single data points or batch-wise privacy preservation through manual configuration of the privacy parameter (ε). In this paper, we propose an adaptive contextual privacy preservation method that analyzes the data attributes required for specific application services, acting as context. It then identifies sensitive attributes and adaptively selects the value of ε for each data attribute to maintain a balance between privacy and service requirements. The proposed approach was evaluated using power consumption and solar power generation datasets. The results show that the proposed approach dynamically selects the privacy parameter for each data attribute. Moreover, the original and anonymized data were fed into the prompt to assess the textual responses generated by LLM. The results show that our proposed approach achieved an average degree of semantic similarity score of 94.5% for power consumption data and 95.23% for solar power generation data.

CCS CONCEPTS • Security and privacy • Security services • Pseudonymity, anonymity and untraceability

Additional Keywords and Phrases: Large Language Models, Privacy Preservation, Differential Privacy, Time Series Data

ACM Reference Format:

Ubaid Ur Rehman, Musarrat Hussain, Tri D.T. Nguyen, and Sungyoung Lee. 2023. Let's Hide from LLMs: An Adaptive Contextual Privacy Preservation Method for Time Series Data. In 2023 6th Artificial Intelligence and Cloud Computing Conference (AICCC) (AICCC 2023), December 16–18, 2023, Kyoto, Japan. ACM, New York, NY, USA, 14 pages.

1 INTRODUCTION

The rapid advancement of IoT has raised privacy concerns because it continuously transmits time-series data that includes sensitive information. The acquired data are either stored in data repositories managed by the data curator for retrieval as needed or utilized by domain-specific applications to provide personalized services or decision-making. Usually, data curators are considered trustworthy and manage the data received from data sources in a secure and organized manner. However, with the emergence of the zero trust security model, which relies on the principle of "never trust, always verify," the concern arises regarding what happens if the data curator is untrusted. This leads to privacy concerns because the data managed by the data curator includes sensitive and personally identifiable information, and any leakage or mishandling may lead to serious consequences. Therefore, some privacy mechanisms need to be deployed alongside authentication and authorization for data curators to ensure data protection, compliance with the General Data Protection Regulation (GDPR), and the Health Insurance Portability and Accountability Act (HIPAA), and to mitigate associated risks.

Another major concern is sharing the acquired time-series data with third-party services, such as data analysts, service providers, and Large Language Models (LLMs). These services utilize data-hungry machine learning systems, expert heuristics, and statistical methods to analyze the data, extract insights, and process the data according to the target requirements for making informed decisions. Therefore, the need for privacy and compliance with data governance is crucial when sharing data with these third-party services. Specifically, the widespread adoption of LLMs by different domain-specific applications has raised concerns regarding the potential leakage of sensitive information. LLMs interact in natural language, answer questions, and assist users with various tasks. To retrieve specific responses from LLMs, domain-specific applications feed the time-series data into prompts for in-context learning and retrieve relevant responses, leading to privacy concerns. Carlini et al. in [1] demonstrated an attack on Generative Pre-trained Transformer (GPT-2) to extract verbatim text sequences and personally identifiable information used to train GPT-2. Therefore, a privacy preservation approach is needed to ensure a balance between privacy and the required service.

In this study, we have proposed an adaptive contextual privacy preservation method for time series data using differential privacy. The proposed approach addresses the two privacy concerns, including the untrusted data curator and data handling with third-party services. For each service, it identifies the context by grouping the required data, then identifies sensitive data attributes and adaptively allocates the privacy parameter for each attribute. It then computes and adds Laplace noise to the targeted time-series data to ensure differential privacy. We have evaluated our proposed approach with two datasets to assess contextual privacy preservation and dynamic allocation of privacy parameters. The results show that the proposed approach efficiently identifies the context and adaptively allocates the privacy parameter. To ensure the privacy preservation of time-series data in LLM, we have created prompt templates, inserted the original and

noisy data, and acquired responses from LLM given the prompt. We then compared the responses received using original and noisy prompts, which showed a very low impact of changes on the generated responses. Therefore, we can utilize the noisy prompt to obtain responses from LLM instead of considering the original data due to privacy concerns.

The rest of the paper is organized as follows: Section 2 provides an overview of related work. Section 3 briefly describes our proposed adaptive contextual privacy preservation method. The evaluation of our proposed approach based on two datasets and its evaluation with LLM is presented in Section 4. Finally, Section 5 summarizes the proposed approach, its limitations, and sets future directions.

2 RELATED WORK

In this section, we describe the most recent and relevant literature related to our proposed methodology. We have identified eight studies, among which six studies have considered LLMs, specifically privacy preservation mechanisms for named entity types, but did not consider time series data with LLMs. However, two of the studies have considered privacy preservation techniques but not from the perspective of LLMs. In this study, we bridge this gap and consider privacy preservation for time-series data along with LLMs. The detailed descriptions of the existing approaches are as follows.

2.1 Privacy Preservation Techniques Considering LLMs

In this section, we describe the existing approaches developed or applied in the context of LLMs. Yermilov et al. in [2] analyzed the effectiveness of pseudonymization techniques using various datasets and models used for text classification and summarization. The authors emphasized identifying a suitable pseudonymization method for LLMs that can strike a balance between privacy and utility. The proposed approach focused on named entity types (person, location, and organization) but did not consider the assessment of time series data.

In [3], the authors analyzed the responses generated from LLMs for input copying and regurgitation. For this purpose, they created three prompts that comply with privacy regulations and protect sensitive information from leakage to retrieve responses from LLMs. The authors concluded that only prompts compliant with privacy regulations cannot guarantee privacy preservation. Therefore, an effective privacy preservation method can reduce the risk of information leakage to LLMs.

Kim et al. [4] proposed a probing tool to create awareness about the leakage of Personally Identifiable Information (PII) to LLMs. The approach used masked templates and acquired responses from LLMs. If the retrieved information resembled the ground truth, it indicated a high privacy risk to PII. However, the approach did not propose a privacy preservation mechanism to prevent the leakage of PII.

Chen et al. in [5] proposed an anonymization technique to protect PII information in a prompt by substituting it with filler or a mask. The proposed approach only considered named entity types and is not suitable for time series data.

In [6], the author proposed a data curator who collects data from different stakeholders and applies masking to ensure privacy. They then used the masked data to extract valuable insights from LLMs. The approach identified the named entity types from the aggregated data, masked them, and provided that data in prompts to retrieve a response. The approach by South et al. is not suitable for time series data.

Beyer et al. in [7] preserved the privacy of quasi-identifiers (age, marital status, or occupation) and proposed a prompting technique to engage LLMs in generating responses between a hypothetical user and a virtual assistant. The approach required an expert to annotate the quasi-identifiers dataset, which is a time-consuming process and requires specialized professionals.

2.2 Privacy Preservation Techniques Considering Time Series Data

In this section, we describe the methods or techniques proposed to preserve the privacy of time-series data. Katsomallos et al. in [8] proposed landmark privacy that quantifies the privacy loss under temporal correlation. The proposed approach preserves the actual timestamp of the landmarks but only considered the timestamp, not the actual value at the corresponding timestamp.

In [9], the author proposed a data curator who collects time-series data from IoTs and, based on the service request, tailors it to meet the requirements and ensure that PII is not shared. This approach did not consider the privacy concern of an untrusted data curator.

3 ADAPTIVE CONTEXTUAL PRIVACY PRESERVATION METHOD

We have identified from the existing literature that the data curator is usually considered a trusted resource, and data from physical resources can be directly stored and managed by the data curator. However, if the data curator itself is untrusted, then data privacy is at risk. In our proposed approach, we have considered two privacy concerns, as shown in Figure 1.

The first concern highlights that when data sources acquire data and share it with the data curator, no privacy preservation techniques are applied. The data curator can analyze and extract behavior patterns accordingly. Therefore, we need to eliminate the assumption of considering the data curator as a trusted party and take necessary measures accordingly.

The second concern is the sharing of data with targeted services. Usually, the acquired data can be utilized by data analysts, service providers, and, more recently, Large Language Models (LLMs). Data analysts can identify patterns, behaviors, insights, and correlations between different attributes. Service providers can utilize machine learning, expert heuristics, and statistical methods to provide relevant domain-specific personalized services. Additionally, with the popularity of LLMs and their adoption by different service providers, such data are now inserted into predefined prompt templates to provide human-interpreted text in the form of performance reports, health reports, and time series insights. Therefore, sharing data with these third-party services raises significant privacy concerns, especially in the domains of healthcare, energy management, and performance management.

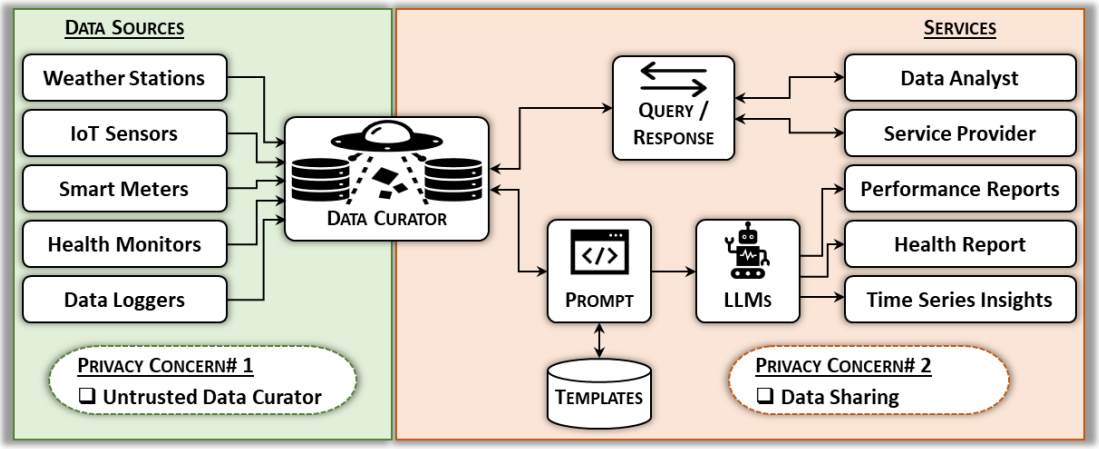

Figure 1: Privacy Concerns in terms of Untrusted Data Curator and Data Sharing

Given the issues of an untrusted data curator and data sharing privacy, we have proposed an adaptive contextual privacy preservation method. This method is based on the concept of a zero-trust model, which eliminates the assumption of trust in any resource or communicating entity. Figure 2 illustrates the conceptual workflow of our proposed methodology. The details of each component are described as follows.

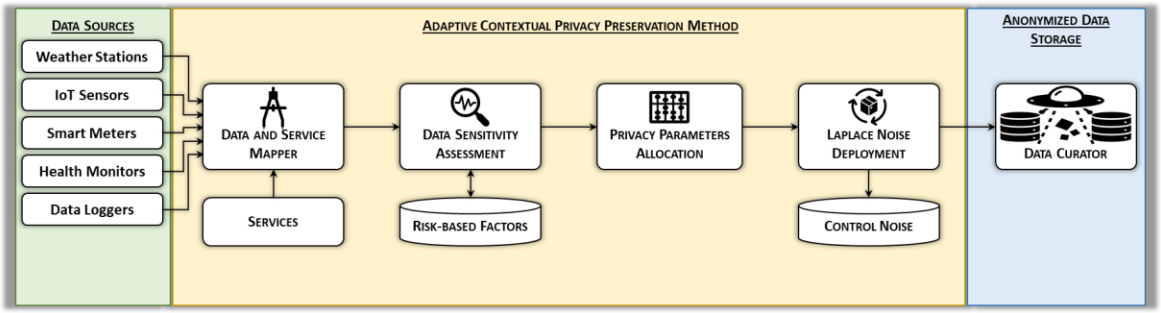

Figure 2: Adaptive Contextual Privacy Preservation Method

3.1 Data Sources

The data sources consist of various physical or virtual resources that can assess their surroundings and acquire data. Since the focus of our proposed approach is on privacy preservation for time series data, we have specified the types of resources that can acquire such data. These include weather stations, IoT sensors, smart meters, health monitors, and data loggers.

3.1.1 Weather Stations.

Weather station data includes information on temperature, humidity, wind speed, and atmospheric pressure, which is used for weather forecasting. Weather station data plays a crucial role in proactively managing power consumption.

3.1.2 IoT Sensors.

IoT sensors encompass a variety of sensor types designed for different purposes, such as ambient sensors for environmental conditions, motion sensors for occupancy detection, proximity sensors for range identification, and biometric sensors for security purposes. Data acquired from IoT sensors is typically very sensitive and requires proper handling to avoid privacy risks.

3.1.3 Smart Meters.

Smart meter data usually consists of consumer information related to electricity, gas, and water usage. Analyzing such data can help identify user consumption behavior and provide cost benefits for smart energy management. Therefore, the privacy preservation of such data is crucial in the energy management domain.

3.1.4 Health Monitors.

Health monitors include data from wearables and medical devices, which are directly related to personal health information and may contain personally identifiable information. This data is used by different healthcare applications to provide various services, such as medication adherence and wellness-related decisions.

3.1.5 Data Logger.

Data loggers store information over time that can be used for anomaly detection, security information, event management, and disaster management. They typically contain very sensitive records and require proper security and privacy measures.

3.2 Data and Service Mapper

The data and service mappers acquire two types of inputs: (i) from data sources and (ii) from services. As illustrated in Figure 1, the data sources include weather stations, IoT sensors, smart meters, health monitors, and data loggers. Similarly, the services include data analysts, service providers, and LLMs. The data and service mapper acquire this information and map it accordingly.

3.2.1 Data Analyst.

Data analysts are interested in identifying patterns, behaviors, insights, and correlations between different attributes. Therefore, the data and service mapper maps the data analyst with each resource available in the data sources.

3.2.2 Service Provider.

The services provided depend on the types of services, resources, and operational processes. It relies on the integration of our proposed approach with service provider applications. In the case of healthcare and

medication adherence applications, data from IoT sensors and health monitors can be provided. For anomaly detection and prevention, the service provider can gain access to all types of data. Similarly, in the case of energy storage system scheduling and energy price estimation, the service is mapped with data from smart meters, IoT sensors, and weather station data.

3.2.3 Large Language Models (LLMs).

LLMs understand natural language and generate responses based on given prompts. The prompt plays a crucial role because it helps LLMs understand specific queries and generate responses accordingly. Therefore, the prompt needs to contain specific information to provide a basic context to LLMs for generating relevant reports. The data and service mapper maps the data with the required information by the prompt to generate a specific textual report.

For example, in the case of a performance report, the prompt may require access to all types of data to provide trend analysis, narrative generation, and recommendations. In the case of a health report, the prompt may need access to vital signs, physical activities, and medical history. Similarly, for time series insights generated from LLMs, the prompt needs to provide historical data for effective response generation.

3.3 Data Sensitivity Assessment

The data sensitivity assessment involves acquiring data that has been mapped with services from the data and service mapper. It then identifies attributes that may have privacy constraints, such as vital signs, medical history, and smart meter data. We have adopted a risk-based approach for analyzing data sensitivity, which is a rule-based method that includes expert heuristics in the form of rules to categorize each attribute as sensitive (1) or non-sensitive (0).

After processing the data, each attribute is assigned a flag. For instance, vital signs assigned with 1 are categorized as sensitive, while wind speed assigned with 0 is categorized as non-sensitive. It is possible that one attribute can be considered very sensitive for a specific service, but the same attribute may be considered non-sensitive for another type of service. Therefore, the risk-based approach takes into account all these constraints, including the targeted services, and assigns sensitivity tags accordingly.

3.4 Privacy Parameters Allocation

Privacy parameter allocation is an important step in our proposed solution. The context about a specific service and sensitive attributes has already been identified in the previous steps. Privacy parameter allocation adaptively selects parameters in such a way that it ensures a proper balance between privacy and service requirements. This ensures that the transformed privacy-preserved data does not degrade the accuracy of the targeted service.

Since our proposed approach is related to time series data, we have used a statistical privacy-preserving technique called differential privacy. This technique adds controlled noise to each data point based on a Laplace or Gaussian distribution, ensuring that individual data points cannot be re-identified. We have used differential privacy with a Laplace distribution to account for the heavy-tailed behavior of time series data, which may have occasional extreme values. Differential privacy with Laplace distribution depends on the privacy parameter (ε), sensitivity (Δf), and location parameter (μ).

3.4.1 Privacy Parameter (ε).

The privacy parameter (ε) quantifies the level of differential privacy. A small ε value means more noise is introduced, making it harder for adversaries to distinguish, leading to stronger privacy. A larger ε value means less noise and weaker privacy. Our proposed approach adaptively selects the value of ε from the set [1, 10, 100, 1000], which corresponds to [Strong Privacy, Medium-High Privacy, Medium Privacy, Low Privacy], respectively. The method analyzes each attribute with its sensitivity flag and selects the appropriate ε value for each attribute, ensuring that the cumulative privacy-preserved data can be used by each service for performing specific tasks. For example, for a dataset with three attributes, two of which are highly sensitive, and one with low sensitivity, the approach may allocate ε values of 10 and 100 to the highly sensitive attributes and 1000 to the low sensitivity attribute, resulting in an overall medium level of privacy for the dataset.

3.4.2 Sensitivity (Δf).

Sensitivity (Δf) quantifies the change that occurs when adding or removing a data point from the dataset. It identifies the controlled noise to be added to the query result to achieve differential privacy. Since our proposed approach deals with time series data, which contains numerical values, we define sensitivity as $\Delta f = Maximum_{Value} - Minimum_{Value}$. This equation calculates the difference between the maximum and minimum values in the selected dataset attribute. The difference quantifies the change, where a higher Δf value indicates greater sensitivity and vice versa.

3.4.3 Location Parameter (μ).

The location parameter (μ) specifies the center of the distribution. It adjusts the center of the controlled noise added to the query results. For our proposed approach, we use the same scale of differential privacy, defined as $\mu = {\Delta f}/{\varepsilon}$. A larger μ value means the noise distribution is centered farther away from the query result, resulting in less noisy data and weaker privacy. A smaller μ value centers the noise closer to the query result, leading to more noisy data and stronger privacy.

3.5 Laplace Noise Deployment

After privacy parameters allocation (ε, Δf, μ), Laplace noise is computed and added to the targeted time-series data to ensure differential privacy and maintain data utility. Our proposed approach stores the controlled noise added to each dataset in a repository with a unique identifier. Storing the controlled noise for each dataset ensures that the same privacy preservation mechanism is consistently applied to the specific data in the future.

3.6 Anonymized Data Storage

The data curator acquires the anonymized data and stores it in an organized manner. The transformed data protects individual identities while retaining the statistical properties and patterns of the original data. Therefore, it is suitable for identifying patterns, behaviors, insights, and correlations between different attributes. The service provider can utilize the anonymized data to provide utilities with the same level of decision-making accuracy as the original data. Additionally, the same data attributes can be used by the prompt to generate textual responses and prevent information leakage to the LLMs. In this way, our proposed

approach addresses the privacy concerns related to an untrusted data curator and data sharing with third-party services.

4 EVALUATION

To evaluate the proposed adaptive contextual privacy preservation method, we selected a case study of an energy management system, where the smart meter collects power consumption data from consumers, and the solar energy meter measures the power generated from solar photovoltaic systems. We acquired two publicly available datasets related to power consumption and solar power generation and applied our proposed methodology independently to assess its impact. The details of each dataset are described as follows.

4.1 Power Consumption Data

Power consumption data can be used by adversaries to identify the living behavior of individuals and could potentially lead to burglary if leaked to malicious users. Therefore, a privacy preservation mechanism is required to prevent such information leakage. We acquired domestic power consumption data consisting of 473 data points with four features, including equipment, host interface device, date-time, and power consumption. Our proposed approach identifies power consumption as highly sensitive and considers the other three features as having low sensitivity within the domain of the energy management system.

The proposed approach first computes differential privacy by considering ε values of [1, 10, 100, 1000], and then identifies the correlation between the original and noisy data. Based on the results obtained from the correlation analysis, privacy requirements, and service requirements, the proposed approach adaptively selects the data that can be utilized by data analysts, service providers, and LLMs to provide specific services. Figure 3 illustrates the results obtained for each privacy parameter. The proposed approach selected the ε = 100 data as the final anonymized power consumption data, ensuring a balance between privacy and utility requirements.

To assess the impact of anonymized data on service requirements, we used an LLM to generate textual reports using both the original and noisy data of power consumption.

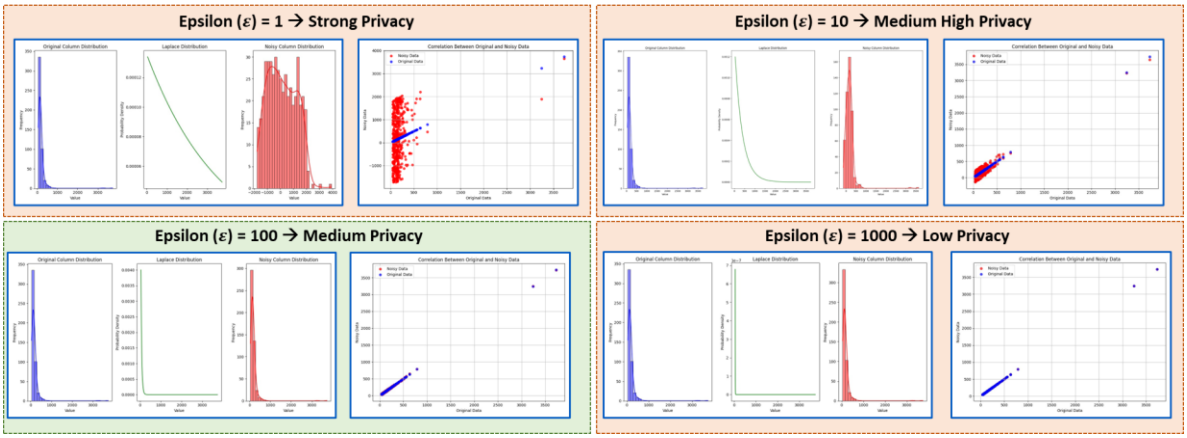

Figure 3: Adaptive Selection of Privacy Parameter (ε = 100) on Power Consumption Data

4.1.1 Assessing the Impact of Anonymized Power Consumption Data.

To evaluate the impact of anonymized power consumption data on textual report generation, we utilized the GPT-2 library from Hugging Face as an LLM. We then created three prompt templates and provided both the original and noisy values to obtain responses from the LLM, as illustrated in Figure 4.

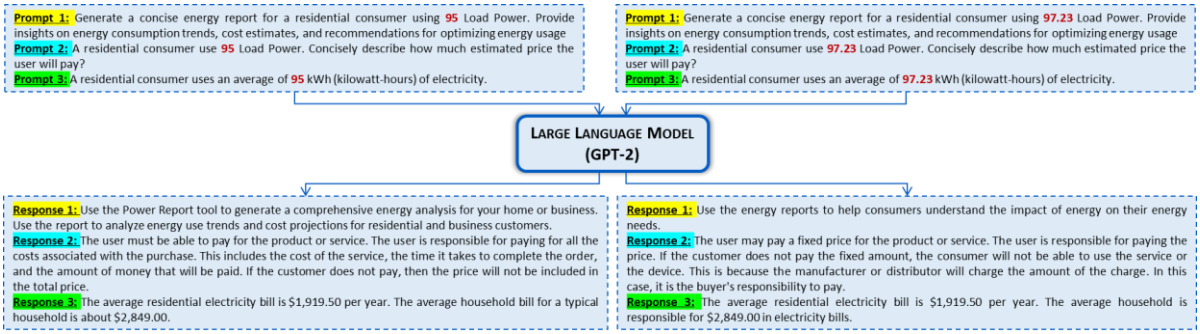

Figure 4: Retrieving LLM Response Using Original and Noisy Power Consumption Data

To compute the similarity between the responses obtained from utilizing the original and noisy power consumption data, we employed a Semantic Textual Similarity (STS) model. This model computes the contextual embedding of each response using a pre-trained Bidirectional Encoder Representations from Transformers (BERT), and subsequently calculates the cosine similarity between the contextual embeddings to obtain the similarity score. Figure 5 presents the similarity scores obtained using STS.

The results show that the value of ε was appropriately selected for the power consumption dataset, achieving an average degree of semantic similarity of 94.5% for these three prompts. Additionally, the generated textual description is dependent on the given prompt template, as illustrated in Figure 5, where the results obtained from prompt 1 and 2 are compared with those from prompt 3.

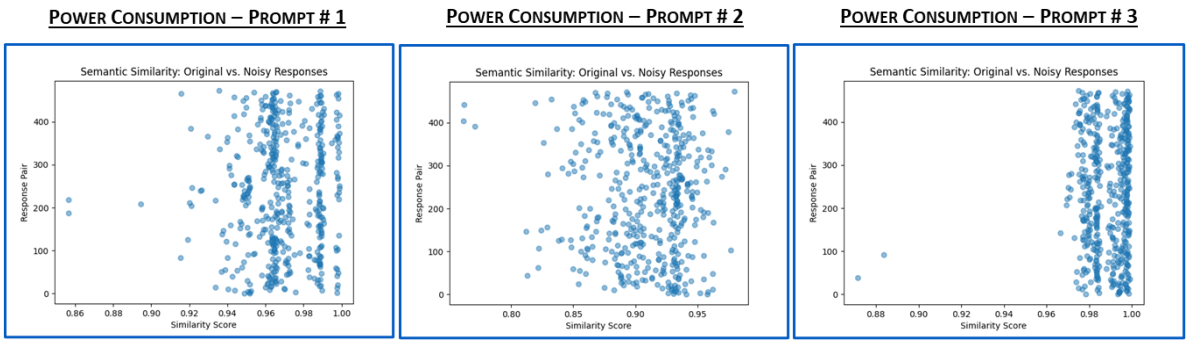

Figure 5: Semantic Textual Similarity Results on Power Consumption Dataset

4.2 Solar Power Generation Data

With the emergence of green energy, consumers become prosumers by producing electricity from photovoltaic sources and then selling the excess energy to utility companies to either generate revenue or reduce utility costs. Energy companies have introduced smart bidding platforms to collect bids from prosumers, consumers, and distributors, using energy trading mechanisms to identify lists of buyers and sellers with cost benefits to meet energy utility requirements. If an adversary obtains information about an individual's generated power, they could potentially compute the financial benefits that the individual could receive from energy trading, which raises privacy concerns.

To address these concerns, we applied our proposed approach to the solar power generation dataset, which consists of 3,465 data points with four features: date, total (kW), maximum (kWh), and minimum (kWh) power generated per hour. Our proposed approach assessed the correlation between the original and noisy attributes after the privacy parameter allocation and then selected the most appropriate value of ε for each attribute, as shown in Figure 6. The proposed approach adaptively selected ε = 1000 for total (kW), ε = 100 for maximum (kWh), and ε = 10 for minimum (kWh). The dynamic selection of ε values was due to the varying impact of each attribute.

Total (kW) was assigned a lower level of privacy because it has a high impact on decision-making, followed by maximum (kWh), and then minimum (kWh). Therefore, our proposed approach considered these constraints to ensure privacy preservation. If the anonymized value significantly deviates from the original value, it can lead to inaccurate results. In this case, the overall privacy preservation of solar power generation is considered to be at a medium level.

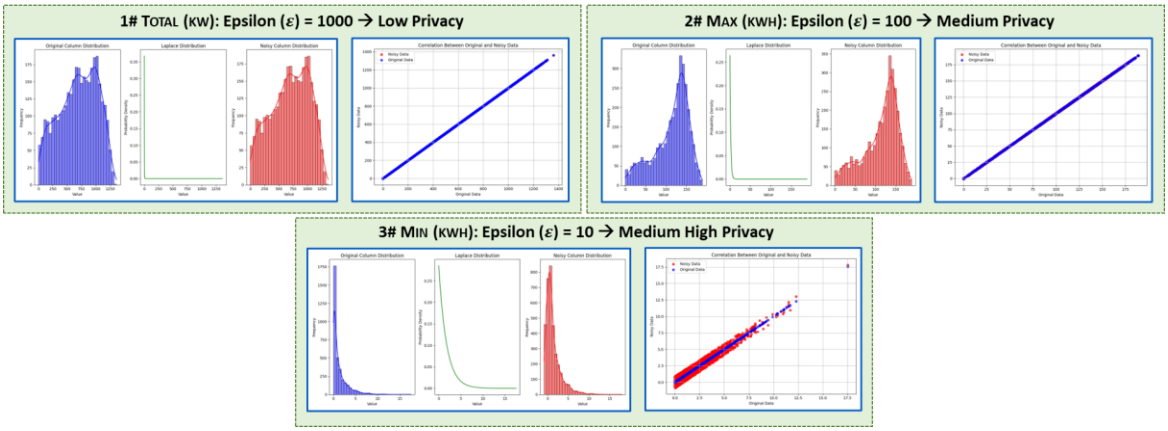

Figure 6: Adaptive Selection of Privacy Parameter (ε = [1000,100,10]) on Solar Power Generation Data

4.2.1 Assessing the Impact of Anonymized Solar Power Generated Data.

We also assessed the impact of anonymized solar power generation data on textual report generation. To do so, we formulated three prompt templates and inserted both the original and noisy values to generate responses from the LLM, as illustrated in Figure 7.

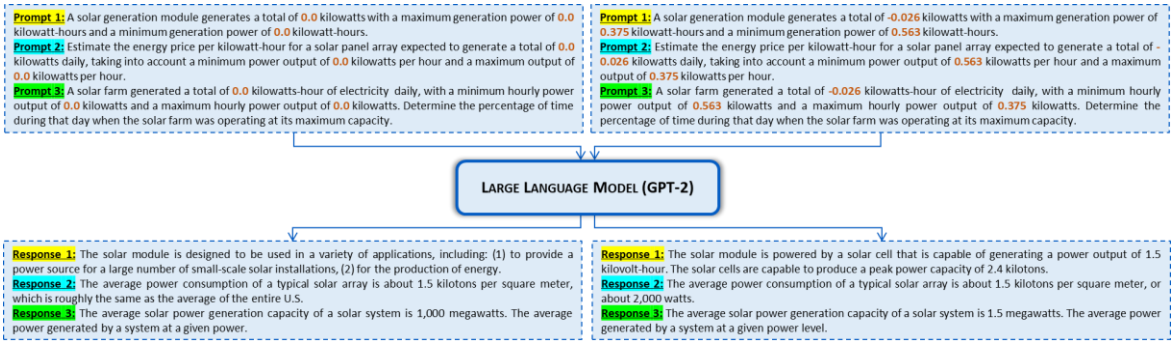

Figure 7: Retrieving LLM Response Using Original and Noisy Solar Power Generation Data

The similarity score was computed using STS between the responses obtained from the original and noisy prompts. Figure 8 illustrates the similarity scores obtained from these three prompts using solar power generation data. The results obtained from the dynamic selection of ε values achieved an average of 95.23% degree of semantic similarity based on these three prompts. Moreover, the prompts included more specific information about the desired report. Therefore, the generated reports were very concise and specific, leading to higher similarity scores in this case.

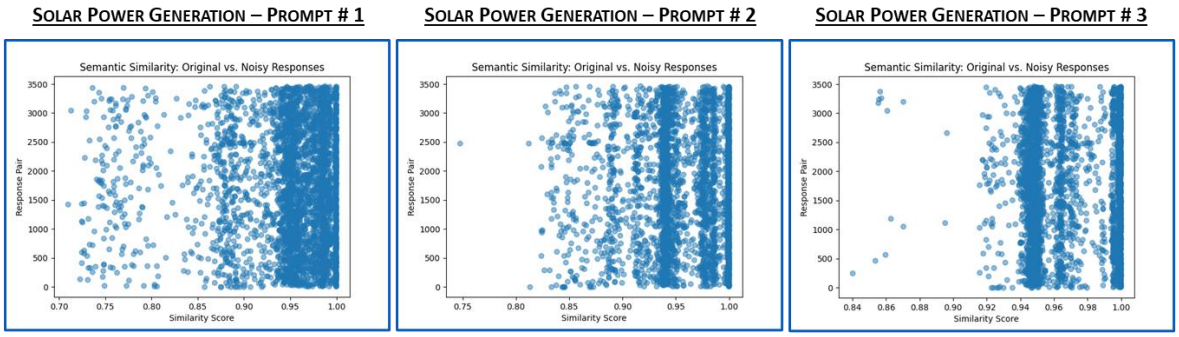

Figure 8: Semantic Textual Similarity Results on Solar Power Generation Dataset

5 CONCLUSION

In this study, we proposed an adaptive contextual privacy preservation method for time series data using differential privacy. Our approach groups data based on the targeted service, identifies sensitive attributes through risk-based factors, and adaptively selects the privacy parameter based on correlation, privacy levels, and service requirements. After privacy parameter allocation, Laplace noise is computed and added to the targeted time series data to ensure differential privacy. Our objective was to eliminate the assumption of trust and ensure privacy preservation during data sharing with third-party services, including LLMs. We evaluated our approach using power consumption and solar power generation datasets, and the results showed that the proposed approach dynamically selects the privacy parameter for each data attribute. Furthermore, we assessed the impact of anonymized data on textual report generation using GPT-2 and computed the STS of responses obtained from original and noisy prompts. Our proposed approach achieved an average degree of semantic similarity score of 94.5% for power consumption data and 95.23% for solar power generation data. We also identified that the generation of textual descriptions is dependent on the given prompt template.

However, our proposed approach has limitations, as it may not be suitable for application areas that require specific values for decision-making. Additionally, the approach is resource-intensive, as it computes the Laplace distribution based on given ε values and selects the most appropriate privacy parameter for each data attribute based on correlation results. In the future, we will address these limitations to enhance our proposed approach and evaluate it with diverse data from different domain applications.

ACKNOWLEDGMENTS

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the Grand Information Technology Research Center support program (IITP-2022-2020-0-01489), the ITRC (Information Technology Research Center) support program (RS-2023-00259004) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation) and by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (IITP-2022-0-00078, Explainable Logical Reasoning for Medical Knowledge Generation), (IITP-2017-0-00655, Lean UX core technology and platform for any digital artifacts UX evaluation).

REFERENCES

[1] Carlini, Nicholas, Florian Tramer, Eric Wallace, Matthew Jagielski, Ariel Herbert-Voss, Katherine Lee, Adam Roberts et al. "Extracting training data from large language models." In 30th USENIX Security Symposium (USENIX Security 21), pp. 2633-2650. 2021.

[2] Yermilov, Oleksandr, Vipul Raheja, and Artem Chernodub. "Privacy-and Utility-Preserving NLP with Anonymized Data: A case study of Pseudonymization." arXiv preprint arXiv:2306.05561 (2023).

[3] Priyanshu, Aman, Supriti Vijay, Ayush Kumar, Rakshit Naidu, and Fatemehsadat Mireshghallah. "Are Chatbots Ready for Privacy-Sensitive Applications? An Investigation into Input Regurgitation and Prompt-Induced Sanitization." arXiv preprint arXiv:2305.15008 (2023).

[4] Kim, Siwon, Sangdoo Yun, Hwaran Lee, Martin Gubri, Sungroh Yoon, and Seong Joon Oh. "Propile: Probing privacy leakage in large language models." arXiv preprint arXiv:2307.01881 (2023).

[5] Chen, Yu, Tingxin Li, Huiming Liu, and Yang Yu. "Hide and Seek (HaS): A Lightweight Framework for Prompt Privacy Protection." arXiv preprint arXiv:2309.03057 (2023).

[6] South, Tobin, Guy Zuskind, Robert Mahari, and Thomas Hardjono. "Secure Community Transformers: Private Pooled Data for LLMs."

[7] Beyer, Franka, Zahra Kolagar, and Darina Gold. "Let's Write Privacy: Survey and Experiment Design on Textual Privacy in Conversation." (2023).

[8] Katsomallos, Manos, Katerina Tzompanaki, and Dimitris Kotzinos. "Landmark privacy: Configurable differential privacy protection for time series." In Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy, pp. 179-190. 2022.

[9] Stach, Christoph. "VAULT: A Privacy Approach towards High-Utility Time Series Data." In Proceedings of the Thirteenth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Nice, France, pp. 27-31. 2019.