PIONEER
ACADEMIC PUBLISHING LIMITED

Journal of Progress in Engineering and Physical Science
ISSN 2709-4006
www.pioneerpublisher.com/jpeps
Volume 2 Number 4 December 2023

Advancements in Encryption Techniques for Enhancing Meteorological Data Security During Catastrophic Weather Events

Gang Du[1]

[1] Jiangsu Meteorological Information Center, Nanjing 210000, China
Correspondence: Gang Du, Jiangsu Meteorological Information Center, Nanjing 210000, China.

doi:10.56397/JPEPS.2023.12.05

Abstract

With the widespread utilization of meteorological data across diverse fields, the imperative for ensuring its security and safeguarding privacy has escalated. Meteorological data encompasses a wealth of sensitive information, including frequency bands and the precise locations of sensing devices. Inappropriate handling of this data may engender profound ramifications for multiple stakeholders. Particularly in the face of severe catastrophic weather conditions, the conundrum of optimizing the analysis and transmission of critical meteorological data within the confines of finite resources and time constraints looms large, demanding immediate attention from researchers. This paper centralizes its focus on the analysis and storage of information derived from common meteorological devices, proposing a priority-weighted encryption strategy. Within this strategy, meteorological data attains the utmost degree of privacy attainment while concurrently improving encryption efficiency, even when faced with the stringent limitations of limited resources and time constraints during severe catastrophic weather events.

Keywords: meteorological data, privacy protection, sensitive information, privacy attainment

1. Introduction

In light of the swift advancements in modern technology, the acquisition, retention, and transmission of meteorological data have grown in frequency and sophistication. Particularly in the forecasting and response to significant catastrophic weather events, such as typhoons, earthquakes, and floods, there is an exigent demand for the swift collection and dissemination of copious volumes of personal and collective data. This is essential to support rescue operations and guarantee the safety of individuals' lives and property. Nonetheless, this data frequently encompasses a significant trove of meteorological privacy information. The challenge at hand is to ensure a swift and precise rescue response while simultaneously safeguarding this sensitive data from unlawful exploitation or disclosure. This has evolved into an immediate and pressing issue requiring resolution.

Meteorological disasters are characterized by their abrupt onset, time sensitivity, and extensive scope. These attributes render traditional data privacy protection methods inadequate in fulfilling the demands for real-

time responsiveness and efficiency during disaster mitigation. Hence, the implementation of efficacious privacy protection strategies, while simultaneously ensuring the fluidity of data, presents not only a technical hurdle but also encompasses a multitude of societal, legal, and ethical considerations.

The collection, storage, processing, and utilization of meteorological data encompass a substantial volume of confidential information and sensitive data, including frequency bands, geographical coordinates, and radio sensing device performance. The inappropriate handling of this information could potentially yield profound repercussions for the welfare of nations, societies, businesses, and individuals. Furthermore, as the domains of meteorological data applications undergo continuous expansion, the concomitant escalation in data security risks becomes increasingly conspicuous. Incidents involving data breaches, tampering, and other security vulnerabilities occur with notable frequency, thereby presenting substantial perils to diverse stakeholders. Consequently, the development of a robust meteorological data privacy protection strategy to safeguard data security emerges as a paramount research imperative.

Within the array of data security protection technologies, encryption technology assumes a pivotal role in fortifying data security, primarily due to its robust security features and practical applicability. Encryption technology leverages intricate mathematical algorithms to convert plaintext data into ciphertext, rendering it decipherable solely by individuals in possession of the decryption key. This methodology significantly mitigates the potential for improper data usage. Encryption technology assumes a pivotal role in enhancing meteorological data security by effectively thwarting interception and tampering during data transmission, thereby safeguarding data integrity and reliability. Furthermore, encrypting meteorological data can prevent unauthorized access during storage, processing, and application phases, thereby ensuring data privacy.

Notwithstanding the substantial contribution of encryption technology to meteorological data security, practical challenges persist. These encompass constraints related to the limited resources available on the devices where encryption algorithms are deployed, the intricacy of algorithm structures, and considerations regarding the efficiency of encryption and decryption processes. These challenges encumber the widespread application of encryption technology in the realm of meteorological data security.

In this context, this paper introduces the Level Priority Protection (LPP) model, specifically designed for the encryption of various data fields within meteorological devices when confronted with major catastrophic weather conditions. Within the constraints of limited resources and time, the paper presents an encryption strategy aimed at maximizing privacy preservation within stringent time limitations.

The primary objective of the LPP model is to optimize the privacy attainment within stringent time constraints. The model is based on the assumption that data encryption during transmission is inherently secure and data storage is adequately protected. This approach ensures the overall security of information transfer while concurrently augmenting encryption efficiency. The combined effect enhances privacy protection while operating within the confines of limited device resources and time limitations.

The remainder of this paper is structured as follows: Section 2 provides a comprehensive review of pertinent literature concerning privacy protection. Sections 3 and 4 delineate the LPP model and the associated algorithms introduced in this study. Following that, Section 5 will present the outcomes of simulation experiments. Ultimately, Section 6 will encapsulate the key findings and conclusions drawn from this paper.

2. Related Work

Amidst the relentless technological advancements, privacy protection methodologies have found extensive application within the realm of meteorology. In the exigent scenario of major catastrophic weather events, the confluence of ensuring prompt and precise responses for rescue operations while concurrently shielding sensitive meteorological data from unauthorized access or disclosure represents a formidable societal challenge.

Vijayarani S, Dhayanand S & Phil M (2015) introduced a robust key management and encryption approach employing attribute-based encryption to grant multiple users authorized decryption capabilities through designated keys.

This method serves as a safeguard against the collusion of multiple users seeking unauthorized access to private information. Mythri G & Jayram B G (2017) presented a framework designed to enhance data access control, with a focus on aspects such as confidentiality, data revocability, dynamic data access, and overall data security. Servers can be local or cloud-based for storing and analyzing system information. Servers can be local or cloud-based for storing and analyzing system information (Al Ameen M, Liu J & Kwak K, 2012; Liang X, Zhang K, Shen X, et al., 2014). Guo C, He GH, Tian Z, et al. (2018) explored the approach of encrypting data prior to its storage in cloud services. While this method effectively mitigates privacy leakage concerns, it introduces supplementary costs related to communication, storage, and computational overhead during data retrieval and query processes. Current solutions fall short of fulfilling user requirements for encrypted searches across multiple sources of meteorological data. A novel, secure, and efficient searchable symmetric encryption scheme is introduced to address this issue. This scheme not only satisfies users' needs for encrypting and searching multi-source data but also guarantees that adversaries cannot access the distribution information of user documents and search results within each data source. Therefore, it can effectively ensure the privacy and security of user data. Guo L, Zhang C, Sun J, et al. (2012, 2013) introduced an identity authentication system founded on privacy-protected attributes, enabling user authentication based on these attributes while concurrently preserving their privacy.

The previously mentioned studies analyze and discuss a range of encryption strategies in various work environments as proposed by previous scholars. Nonetheless, these studies do not incorporate crucial considerations related to privacy weighting and levels. Within distinct meteorological systems, Jacobsson A, Boldt M, and Carlsson B (2016), Savola R M, Savolainen P, Evesti A, et al. (2015), and Tai H, Celesti A, Fazio M, et al. (2015) have proffered risk analysis recommendations and have engaged with privacy security challenges in significant works (Arabo A, Brown I, and El-Moussa F, 2012; Hernández-Serrano J, Muñoz J L, León O, et al., 2018; Weber R H, 2011). Furthermore, Hernández-Serrano J, Muñoz J L, León O, et al. (2018) presented a coherent approach for incorporating the outcomes of privacy-related risk assessments into the entire software development lifecycle, thereby reinforcing privacy security via judicious allocation.

With the ongoing expansion in both the quantity and diversity of meteorological data, privacy concerns have assumed paramount importance within the meteorological industry. This paper centers its focus on the application of apt encryption strategies grounded in privacy weighting factors, particularly within the domain of severe catastrophic weather scenarios. It seeks to establish robust measures for securing the transmission of meteorological equipment information, minimizing the risk of privacy breaches, fortifying the safeguarding of high-privacy-level data, and expediting the encryption of high-level information.

3. Proposed Model

Chapter 2 of this paper introduced the LPP Model and presented an overview of the underlying framework. The subsequent chapter will delve deeper into problem definition.

3.1 Problem Definition

In this paper, the primary research challenge is delineated as the Maximization of Privacy Weight (MPW) problem, which will be expounded upon in Definition 1.

Definition 1 (MPW Problem): The input consists of data types D_i; the data volume for each data type N_{D_i}; the privacy weight $W_{D_i}^n$ for each data type in a low-security mode the computational cost $C_{D_i}^n$ associated with each data type, the privacy weight $W_{D_i}^e$; and the computational cost $C_{D_i}^e$ in a high-security mode, along with a configuration constraint C_s. The desired output is the maximization of privacy weight.

The objective of the problem is to optimize the privacy weight value within temporal constraints.

In Definition 1, the common input data includes data types D_i and the quantity N_{D_i} for each data type.

Moreover, the paper primarily emphasizes the utilization of encryption strategies rooted in privacy weight factors. Consequently, it contemplates two operational modes: the high-security mode and the low-security mode.

Under this working paradigm, data characterized by high privacy concerns and elevated risk can be stored in the high-security mode, whereas public data, such as general information, is allocated to the low-security mode.

1) In the high-security mode, the input data encompasses $C_{D_i}^e$ for each data type, along with the corresponding privacy weight $W_{D_i}^e$.

Computational cost constraints can be any restrictions on

resources or conditions, such as different encryption algorithms $P_{D_i}^e$ or time constraints $T_{D_i}^e$.

2) In the low-security mode, the input data encompasses $C_{D_i}^n$ for each data type and the

privacy weight $W_{D_i}^n$ for each data type, and

similar constraint conditions can be applied.

In this paper, privacy weight is characterized as a metric quantifying the degree of privacy or privacy protection, with the numerical value of the privacy weight positively correlating with the level of privacy protection.

The paper uses P to represent the highest privacy weight achieved after applying the encryption strategy. In the high-security mode, the number of data or data packets for data type D_i is $N_{D_i}^e$, while in the low-security mode, it is $N_{D_i}^n$. Thus, $N_{D_i} = N_{D_i}^e + N_{D_i}^n$. Equation (1) represents the calculation method for P:

$$P = \sum_{s(i)=1} N_{D_i}^e \times W_{D_i}^e + \sum_{s(i)=0} N_{D_i}^n \times W_{D_i}^n \quad (1)$$

The paper uses $COST$ to represent the total computational cost, and C represents the configuration constraint, such as temporal constraints T_s, which are used to represent time constraints. Equation (2) represents the formula for the total computational cost, with the configuration constraint consistent with constraint conditions:

$$COST = \sum_{s(i)=1} N_{D_i}^e \times C_{D_i}^e + \sum_{s(i)=0} N_{D_i}^n \times C_{D_i}^n \quad (2)$$

Where the range of values for C is $0 \le COST \le C^s$.

3.2 Level Priority Protection Model (LPP)

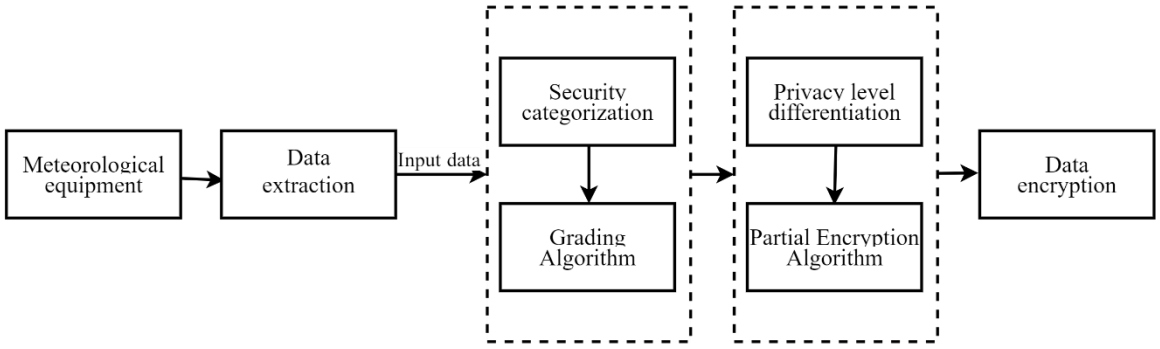

Figure 1. Level Priority Protection Model (LPP)

The structure of the LPP model is shown in Figure 1.

The primary encryption approach outlined in this paper follows these steps: initially, data is identified, and the privacy weight for each data point is established. Subsequently, the data is grouped into distinct tiers based on their respective privacy weights. Generally, data with privacy weights ranging from 0 to 1 are allocated into four levels: Level I (0, 0.1, 0.2), Level II (0.3, 0.4, 0.5), Level III (0.6, 0.7, 0.8), and Level IV (0.9, 1.0). Different levels of encryption measures are then applied to data of varying levels, such as Level I (no encryption), Level II (partial encryption), Level III (partial encryption), and Level IV (full encryption). For low-level data that can be matched with a threat model, one of the data is elevated by one level, giving priority to encrypting higher-level data. For data with long byte lengths but high privacy,

data masking techniques are employed.

The Level Priority Protection Model is designed to optimize the achievement of maximum privacy within a constrained timeframe.

Privacy attainment denotes the device's responsiveness to data encryption in terms of time and resource constraints in typical scenarios. Hence, the extent of data privacy protection within a restricted timeframe is termed "privacy attainment" when the device's computational capacity is restricted.

The principal elements of the model during the encryption process encompass data extraction, Data Privacy Security Rating (DPSR), and the implementation of data masking techniques.

In the first part of LPP, data extraction involves identifying the data, i.e., categorizing data based on security classification. Security classification refers to the privacy weight associated with each data type during the configuration process.

This paper defines CODP identification as the pairing of data or data types that have the potential to compromise an individual's privacy upon review. In essence, when an attacker acquires two data elements or data packets, it may lead to a privacy breach, whereas if the attacker obtains only a single data element or data packet, it would not result in a compromise of the user's privacy. Any pair of data elements or data packets meeting this criterion qualifies as CODP identification. For instance, within meteorological data, station information and rainfall measurement data are two data types that could potentially lead to the exposure of meteorological privacy; therefore, they are considered a paired set.

As outlined in Definition 2, CODP needs to be identified in the initial stage. Paired data for CODP identification is derived from the original dataset, and subsequent adjustments are made to ascertain the pairing of two data elements through collision operations. This paired status resulting from collision operations is referred to as Data Collision (DC).

Definition 2: ∃ two pieces of data or data packets D_1 and D_2. Simultaneously obtaining D_1 and D_2 an compromise a user's privacy, but an attacker accessing one of D_1 or D_2 will not lead to a privacy leak, so D_1 and D_2 are referred to as CODP.

The second phase of LPP, known as Data Privacy Security Rating (DPSR), concerns the determination of privacy importance assigned to each data type during the configuration process. This section will proceed to conduct an in-depth analysis of the pertinent aspects of Data Privacy Security Rating.

Data Privacy Security Rating (DPSR) serves as a metric for evaluating the extent of data exposure risk by taking into account the susceptibility of data to privacy threats and the efficacy of encryption strategies in place. Each data type is assigned a corresponding score, directly mirroring the potential risk of data exposure and its repercussions, particularly in the context of significant meteorological disasters. The outcomes are subsequently classified into four tiers, denoted as Level I (0, 0.1, 0.2), Level II (0.3, 0.4, 0.5), Level III (0.6, 0.7, 0.8), and Level IV (0.9, 1.0). These levels, namely, Level I, Level II, Level III, and Level IV, correspond to the categories of low, low to moderate, medium, and high. In Table 1, you can find an analysis of the overall risk level based on the data's impact and the probability of leakage.

Table 1. Comprehensive Risk Assessment Considering Data Impact and Leakage Probability

Impact \ Leak Probability	Low	Low to Moderate	High
High	Medium	High	Critical
Medium	Medium	Medium	High
Low to Moderate	Low	Low	Medium
Low	Low	Low	Medium

The third component of LPP entails the application of data masking techniques.

When analyzing big data, particularly those containing sensitive information or extensive data byte sizes, it becomes essential to apply data masking in accordance with system

regulations. This ensures that the data can be used for testing, development, and other purposes. In the context of meteorological data, sensitive information like station locations and measurement methods necessitates data masking to effectively safeguard meteorological privacy.

Data masking is a method used to transform data that contains sensitive information into data with reduced or no privacy implications. This typically involves concealing or modifying data elements that could potentially disclose sensitive details, such as station information.

Numerous algorithms are available for data masking, with commonly employed methods encompassing techniques such as masking, rounding, substitution, truncation, among others.

The above description outlines the fundamental procedure of the LPP model, aimed at prioritizing the encryption protection of high-level data. This objective is in line with the imperative of enabling swift and precise responses during severe weather-related disasters, while simultaneously securing meteorologically sensitive data against unauthorized access or disclosure. The subsequent section will elaborate on the threat model.

3.3 Threat Model

In the threat model, we assume that attacker A can monitor all wireless communication. In other words, when data captured is unencrypted or is of importance, A may have visibility into meteorological sensitive data, and this data is only protected at a low-security level.

Assuming the leaked privacy is $< D_p, D_q >$, we use $A \rightarrow < D_p, D_q >$ to denote privacy leakage occurring due to an attack initiated by A.

Assuming the proposed model has been implemented, the transmitted data is paired through DC pairing. This means that at least one data is encrypted or in a higher security state. Encrypted data is represented as $\hat{D}_i$, and, therefore, $< D_p, D_q >$ will have the following state $< \hat{D}_p, D_q > < D_p, \hat{D}_q > < \hat{D}_p, \hat{D}_q >$ after the DC operation. In this state, $A \rightarrow < D_p, D_q >$ cannot be realized. Additionally, some other data operate at higher security levels, depending on the constraint conditions, and thus, the model can effectively handle such threats.

4. Related Algorithms

4.1 Grading Algorithm

The grading algorithm is utilized for data identification and classification, assigning them to various levels based on their respective weights. The primary objective of this algorithm is to ascertain the data or data packets' specific level and subsequently apply distinct encryption methods, including the determination of whether data masking is necessary. The inputs for this algorithm include the M-Table and A-Table, and its output yields a modified M-Table, referred to as M-Table'. Notably, this algorithm incorporates the CODP identification concept outlined in Definition 2, and the A-Table is employed to manage data collisions. Algorithm 4.1 provides the pseudocode for the grading algorithm.

The main stages of Algorithm 4.1 include:

1) Input the initial data weight table M-Table and the pre-defined A-Table.

2) For all data Di in M-Table, find the paired data Dj for Di in A-Table and represent this pairing as Di↔Dj. The pairing rules follow Definition 2.

3) Determine if data Dj is in the mapping table M-Table to decide if the weight needs to be modified. When Dj is in M-Table, the weight value needs to be modified.

4) Compare the weight values of Di data in M-Table. When $0.9 \leq {}^{W_{D_i}} \leq 1.0$, assign an infinite value to ${}^{W_{D_i}}$; when $0.3 \leq {}^{W_{D_i}} \leq 0.8$, assign a finite value to ${}^{W_{D_i}}$; when $0 \leq {}^{W_{D_i}} \leq 0.2$, assign an infinitely small value to ${}^{W_{D_i}}$.

5) After all data is processed and updated, output the modified table M-Table'.

The time complexity of the grading algorithm is T(n) = O(n). This algorithm serves as a precursor to the LPP model and aims to enhance the level of meteorological data privacy protection through priority-weighted encryption in the event of catastrophic weather conditions. The next subsection will introduce partial encryption algorithms.

Pseudocode for the grading algorithm is as follows:

Input: M-Table，A-Table
Output: M-Table'
for ∀ Di in M-Table do
  if Di is in A-Table then
    Get the pairs matching（Di↔Dj）
    if Dj is in M-Table then
     if 0.9≤W_{D_i} Di≤1.0 then
       $W_{D_i} = +\infty$
       else if 0.3≤W_{D_i} ≤0.8
            $W_{D_i} = n$
       else
            $W_{D_i} = -\infty$
       end if
         end if
        end if
      end if
  end for

4.2 Partial Encryption Algorithm

The partial encryption algorithm is designed as a privacy protection strategy that combines time constraints, privacy weight, and byte length. The inputs include M-Table', S-Table, N-Table, byte length threshold Ti, and the output is the data encryption strategy plan P, indicating which data packets need partial encryption. The purpose of this algorithm is to take the M-Table' obtained through the grading algorithm and determine which data should undergo partial encryption, thus reducing the encryption time and improving efficiency. The main steps of the partial encryption algorithm are as follows:

1) Input the time constraints Tc and M-Table, N-Table, and initialize the data set P to an empty set.

2) Use a For loop to set all data segments with byte counts greater than Ti to encrypt any $\frac{\text{total byte count}}{2}$ byte data.

3) Use an If statement to add data packets with W_{D_i} as +∞ to the P set.

4) Output the collection P consisting of data packets from the Di group. All data packets in the P set will undergo encryption.

Pseudocode for the partial encryption algorithm is as follows:

Input: M-Table', N-Table, byte length threshold Ti
Output: P
$P \leftarrow \varnothing$
  if Di is in N-Table then
   for $N_{D_i} > Ti$ then
     $N_{D_i} \leftarrow \frac{N_{D_i}}{2}$
    if $W_{D_i} \in +\infty$ then
      $P \leftarrow D_i$
    end if
      end for
  end if

5. Experiment and Simulation

Given the swift acquisition and dissemination of substantial meteorological data for forecasting and responding to severe weather events, a task vital for safeguarding lives and property, the significance of data encryption in the meteorological domain is abundantly clear. The encryption strategy employed in this study begins by encrypting data in accordance with privacy grades as dictated by societal requirements. Subsequently, for highly sensitive data with extensive byte counts, data masking techniques are employed to decrease encryption time and enhance encryption efficiency, consequently elevating the level of privacy protection.

In this section, we perform a series of experiments and simulations utilizing ground-based observations, upper-air meteorological data, and other relevant sources. These experiments are primarily focused on the comparative analysis of encryption algorithms from two distinct perspectives:

The first approach involves encrypting data packets based solely on their individual weights, without regard to their influence on weight distribution during execution.

The second approach focuses on encrypting data packets according to their contribution to the weight coefficient within a designated unit of time. This method determines encryption quality by evaluating the weight ratio, which represents the proportion of encryption weight

in relation to the total weight.

In the simulation experiments, the objective is to optimize privacy attainment within a constrained time frame.

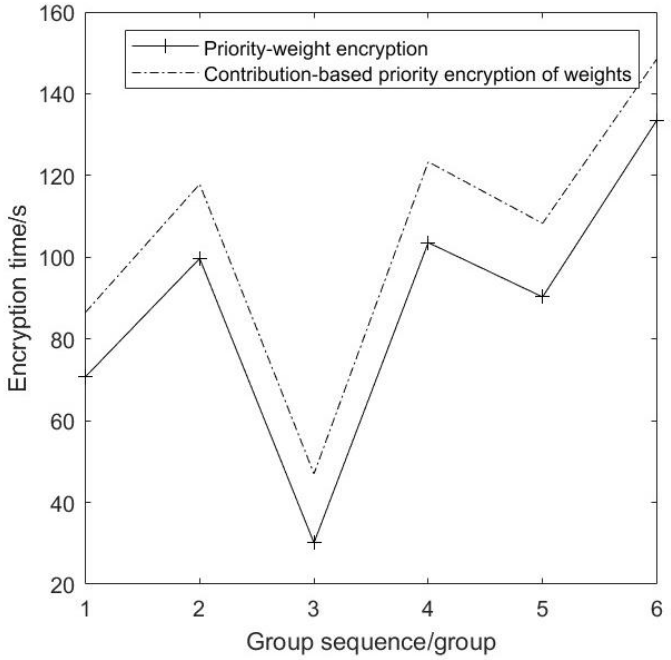

Figure 2. Comparative Time Analysis of Two Encryption Methods for High-Level Data under the RSA Algorithm: A Study across Six Data Groups

Figure 2 compares the time required to prioritize the encryption of data with weights of 0.5 or higher in two different ways under the RSA encryption algorithm. It is evident from the figure that encrypting data based on the order of data weight allows the encryption of high-weight data in a shorter time, ensuring that meteorological privacy is not easily compromised. Lower privacy level data carries less risk, aligning with the encryption philosophy presented in this paper.

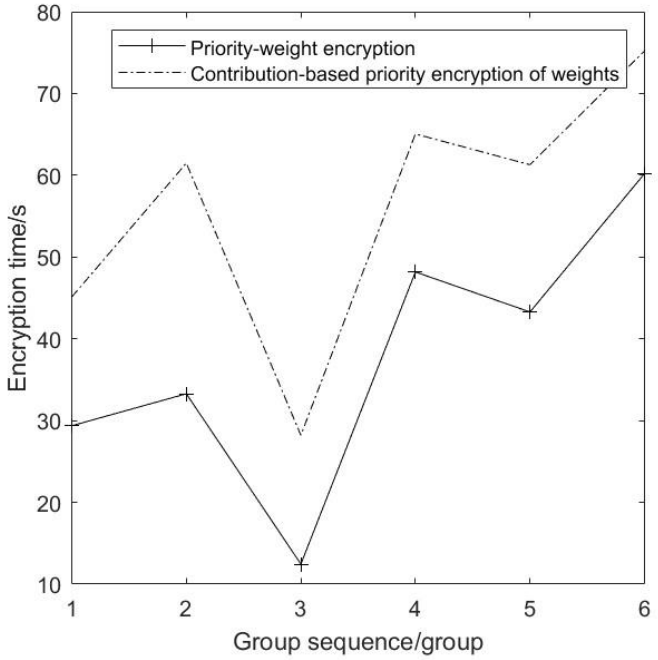

Figure 3. Encryption of High-Level Data, Time Comparison for Two Encryption Approaches under the RSA Algorithm (Incorporating Masking Techniques)

Figure 3 builds on the encryption approach in Figure 2 by adding masking techniques. The results are clear in the figure: the execution time for encryption is significantly reduced, especially for high-byte data. After applying masking techniques, many redundant and critical data are processed, resulting in improved encryption protection.

In the normal data encryption scenario, the addition of data masking techniques not only enhances data privacy protection but also reduces encryption time, improving encryption efficiency.

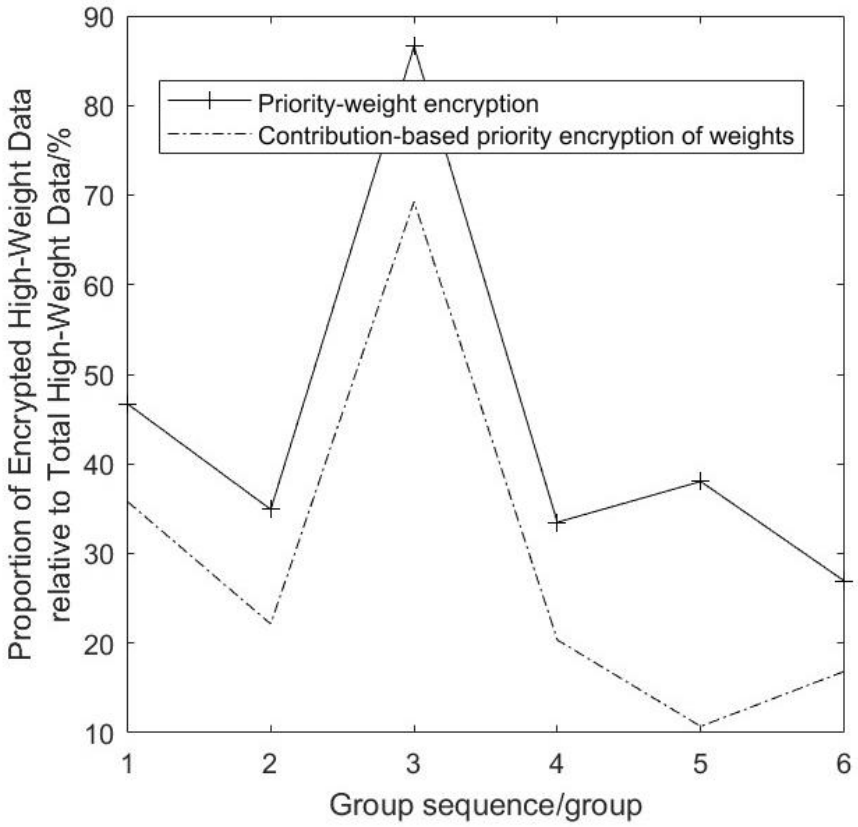

Figure 4. Weight Ratio of Encrypted Data Achieving Privacy Weights of 0.6 and Above within 40 Seconds

Figure 4 shows the proportion of data with privacy weights of 0.6 and above within the high-weight data (all data with weights of 0.6 and above) within 40 seconds.

It can be found that the priority of encryption according to the weight can give priority to the protection of high privacy data, aligning with the privacy protection concept of meteorological data in the context of catastrophic weather events, and to a greater extent ensure that meteorological privacy is in a highly protected state. The experiment is constrained by time, and the results demonstrate that high privacy data can not only be prioritized but also encrypted in a shorter time, enhancing encryption efficiency and significantly reducing the threat of high privacy data leakage.

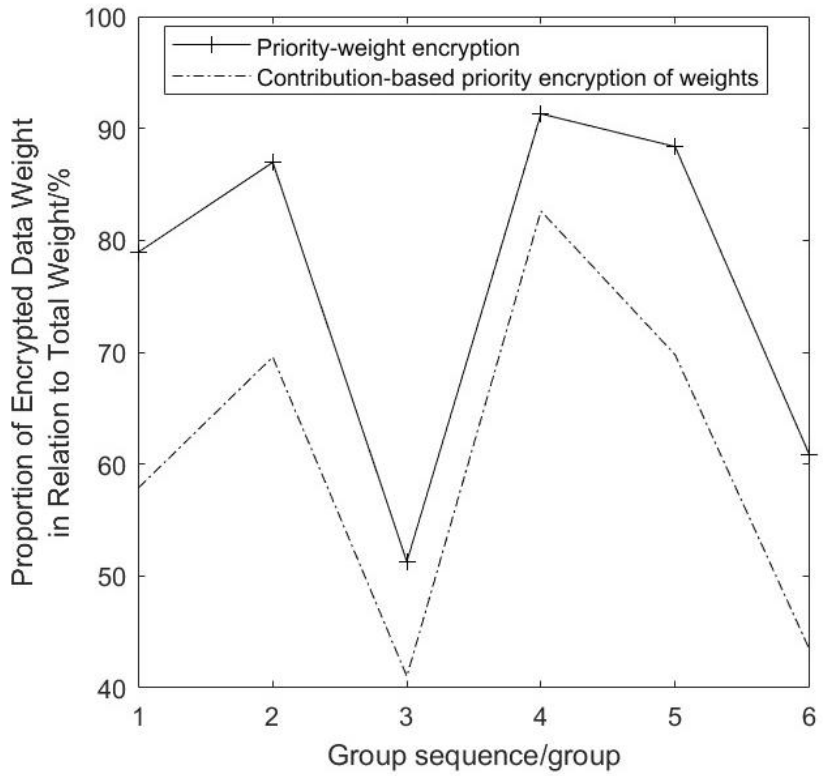

Figure 5. Weight Ratio of Encrypted Data to Total Weight within 40 Seconds

Figure 5 shows the proportion of data with privacy weights of 0.6 and above within the total data weight within 40 seconds when encryption is performed based on the contribution of weight within a unit time. This approach allows high-weight data to be encrypted in a shorter time but is not suitable for the privacy protection of meteorological data in the context of catastrophic weather events. When data has high weight and a large byte count, the contribution value of that data's weight is not necessarily high. In meteorological data, many high privacy data also have high byte counts. Therefore, the weight-prioritized encryption approach can better protect meteorological privacy.

6. Conclusion

Building upon the foundational premise of this paper, the research direction extends beyond mere confidentiality assurance for meteorological data. It is aimed at fortifying the privacy of meteorologically sensitive data within the constraints of limited device resources and time, particularly in the context of severe weather events. The simulations conducted above compellingly illustrate the substantial efficacy of priority-weight encryption in safeguarding the privacy of meteorological data during catastrophic weather conditions. This approach effectively prioritizes the encryption of highly sensitive data, supplemented by masking techniques, leading to reduced execution time and heightened encryption efficiency. Consequently, it significantly mitigates the risks associated with privacy breaches. Within the framework of the Limited Privacy Preservation (LPP) model, it maximizes privacy attainment within the constraints of restricted resources and time, thereby augmenting the overall efficacy of privacy protection.

Reference

Al Ameen M, Liu J, Kwak K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of medical systems*, *36*(1), 93-101.

Arabo A, Brown I, El-Moussa F. (2012). Privacy in the age of mobility and smart devices in smart homes. 2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing. *IEEE*, 819-826.

Guo L, Zhang C, Sun J, et al. (2012). PAAS: A privacy-preserving attribute-based authentication system for eHealth networks. 2012 IEEE 32nd International Conference on

Distributed Computing Systems. *IEEE*, 224-233.

Guo L, Zhang C, Sun J, et al. (2013). A privacy-preserving attribute-based authentication system for mobile health networks. *IEEE Transactions on Mobile Computing, 13*(9), 1927-1941.

Guo C, He GH, Tian Z, et al. (2018). Research and Development of Searchable Symmetric Encryption Schemes for the Security of Meteorological Data. *Advances in Meteorological Science and Technology, 8*(01), 85-91.

Hernández-Serrano J, Muñoz J L, León O, et al. (2018). Privacy risk analysis in the IoT domain. 2018 Global Internet of Things Summit (GIoTS). *IEEE*, 1-6.

Hernández-Serrano J, Muñoz J L, León O, et al. (2018). Privacy risk analysis in the IoT domain. 2018 Global Internet of Things Summit (GIoTS). *IEEE*, 1-6.

Jacobsson A, Boldt M, Carlsson B. (2015). A risk analysis of a smart home automation system. *Future Generation Computer Systems, 56*, 719-733.

Liang X, Zhang K, Shen X, et al. (2014). Security and privacy in mobile social networks: challenges and solutions. *IEEE Wireless Communications, 21*(1), 33-41.

Mythri G, Jayram B G. (2017). Feature based Encryption for Data Privacy and Access Control for Medical application. 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC). *IEEE*, 175-179.175

Savola R M, Savolainen P, Evesti A, et al. (2015). Risk-driven security metrics development for an e-health IoT application. 2015 Information Security for South Africa (ISSA). *IEEE*, 1-6.

Tai H, Celesti A, Fazio M, et al. (2012). An integrated system for advanced water risk management based on cloud computing and IoT. 2015 2nd World Symposium on Web Applications and Networking (WSWAN). *IEEE*, 1-7.

Vijayarani S, Dhayanand S, Phil M. (2015). Kidney disease prediction using SVM and ANN algorithms. *International Journal of Computing and Business Research (IJCBR), 6*(2).

Weber R H. (2011). Accountability in the Internet of Things. *Computer Law & Security Review, 27*(2), 133-138.