electronics

MDPI

Article

An Efficient Encryption Algorithm for the Security of Sensitive Private Information in Cyber-Physical Systems

Xiaogang Zhu [1], Gautam Srivastava [2,3] and Reza M. Parizi [4,*]

[1] School of Software, Nanchang University, Nanchang 30029, China; zhuxiaogang@126.com
[2] Department of Mathematics and Computer Science, Brandon University, Brandon, MB R7A 6A9, Canada; srivastavag@brandonu.ca
[3] Research Center for Interneural Computing, China Medical University, Taichung 40402, Taiwan
[4] College of Computing and Software Engineering, Kennesaw State University, Kennesaw, GA 30144, USA
[*] Correspondence: rparizi1@kennesaw.edu

Received: 4 September 2019; Accepted: 19 October 2019; Published: 25 October 2019

Abstract: The new developments in smart cyber-physical systems can be shown to include smart cities, Internet of things (IoT), and for the most part smart anything. To improve the security of sensitive personal information (SPI) in cyber-physical systems, we present some novel ideas related to the encryption of SPI. Currently, there are issues in traditional encryption methods, such as low speed of information acquisition, low recognition rate, low utilization rate of effective information resources, and high delay of information query. To address these issues, we propose a novel efficient encryption algorithm for the security of incremental SPI. First, our proposed method analyzes user information resources and determines valid data to be encrypted. Next, it uses adaptive acquisition methods to collect information, and uses our encryption method to complete secure encryption of SPI according to the acquisition results. Our experimental analysis clearly shows that the algorithm effectively improves the speed of information acquisition as well as effective information recognition rate, thus enhancing the security of SPI. The encryption model in turn can provide a strong guarantee for user information security.

Keywords: incremental data; privacy information; security; encryption; efficient algorithms; cyber-physical systems; CPS

1. Introduction

As users of smart devices, we have witnessed advancements in systems that are Internet based, which have created many different new avenues and challenges. The term cyber-physical systems (CPS) was first used in the mid-2000s, with the onset of importance given to interactions between systems that are connected to each other and also to the real-world we live in. CPS can be seen more as a thematic subject than as a disciplinary topic. Networked Physical Systems refers to the synchronization between computer information systems and Internet systems, the synchronization and interaction of information between computer process and physical process, and the real realization of object-to-object through the synchronization and interaction of computer calculation, Internet information transmission and industrial operating system control. Object-to-object, human-to-human three-dimensional integrated network information service. At present, network physical systems are mainly used in large-scale industrial production, medical aid system, engineering system and traffic intelligence system.

CPS can be defined as the direct intertwined connections between networks, computing, and processes that are physical in nature. The connections occur as network systems and embedded systems control and monitor processes. From this, built in feedback loops where processes directly affect computations and vice versa are kept track of. The promise of such systems is endless, with both societal and economic ramifications that have not yet been fully realized. We have noticed major financial investments worldwide to develop this technology further and in parallel major research efforts in the newly developed field. Building on both embedded systems and Networked Physical Systems directly, CPS can integrates the dynamics of physical processes with those of both networking and software, providing the necessary abstractions, design, and analysis techniques needed to further their very nature. As CPS are transmitting a myriad of different types of data back and forth between networks, computing resources, and physical hardware, it becomes important to realize that the need for efficient encryption algorithms in CPS exists.

Lately, with the increase in CPS, we have also seen rapid development of information (data) resource sharing. However, the security problems of private information has also appeared. Private information encryption is the symbol of the times and the only way to update and develop secure information sharing. To protect a user's security, it is necessary to encrypt and protect sensitive personal information (SPI), as shown in [1,2]. Currently, users are becoming more concerned with the privacy of their information as opposed to just the novelty of the application being used [3]. Therefore, the secure encryption of SPI is an inevitable requirement of the future development of information sharing and storage [4,5]. SPI encryption has become a recent trend with the development of new information sharing and storage techniques for the future.

Research on encryption algorithms to be used on SPI is an effective way to protect users' privacy. It has piqued the interest and attention of experts and scholars in this field, and achieved some effective research results. Moreover, as indicated earlier, with SPI potentially flowing freely in CPS based networks, the need for the security of such information to be preserved is mandatory and can be provided through our work presented here. Our novel encryption algorithm looks to solve the following shortcomings of current encryption algorithms:

- low-speed data acquisition speed
- low data recognition rate
- effective utilization of resources
- delays in data queries using traditional methods

Before encrypting data, our algorithm analyzes user data resources and encrypts the data according to the analysis results gauging the type of data involved. This effectively solves the problem of data query delays caused by traditional methods in encrypting large amounts of data by only encrypting data that needs enhanced security and privacy. To solve the problem of low data recognition rate and effective utilization of resources, an interference quantification method is used (described later) to determine the location of specific data after the data are encrypted. The experimental results show that the proposed algorithm effectively solves the shortcomings of traditional methods, and can protect a users' privacy and information security. Traditional methods need a lot of manual intervention when encrypting information, and the degree of automation is low. Combining with the analysis of users' private data resources, this paper uses an adaptive data collection method to collect SPI, which can improve the degree of automation of information encryption.

Paper Organization

The rest of the paper is organized as follows. In Section 2, we give a thorough survey of related work to the research presented here. We then present our proposed secure encryption method and its inner workings in Section 3. Our experimental comparison analysis is presented in Section 4. Finally, Section 5 gives some concluding remarks.

2. Related Work

Recently, encryption of personal information has been studied in depth as an effective way to solve the issues with SPI [5]. It has drawn the attention of experts and scholars in many fields, and has resulted in several strong methods.

In [6], Zhang et al. proposed a dual encryption reversible concealment algorithm for real-time network information based on chaotic sequences. The two kinds of scrambling methods are used to double encrypt the network information. For the first time, the chaotic sequence encryption algorithm is used to globally scramble the network information location. The second time, based on another set of chaotic sequences, the 0 bit and 1 bit of the target pixel value are again scrambled to ensure that the selected explicit (dense) attack can be defended. In this domain, the pseudo pixel is constructed by using the information to be embedded to replace the target pixel, thereby realizing rapid embedding of information. The embedded information is directly extracted from the ciphertext information according to the key calculation. After the receiver decrypts the information, each bit data of the target pixel is extracted to recover the original network information, thereby realizing reversible information hiding under double encryption. The experimental results show that the algorithm has the advantages of fast and efficient information embedding and large capacity. However, since the problem that some information can be shared is not considered, the algorithm has the problems of low security information recognition rate and high information query time delay.

In [7], Solomon et al., aiming at the problem that the current algorithm's anti-deciphering ability is not high, proposed a network privacy protection digital information encryption technology based on homomorphic symbol frequency detection. First, the digital information encryption key structure of the network privacy protection object is constructed. Then, the encoding design of encryption and decryption is carried out, which uses the homomorphic symbol frequency detection to perform key optimization of digital encryption to improve the anti-deciphering level. Finally, a simulation experiment was conducted. The delay results show that the digital information encryption technology makes the encryption depth higher, and the deciphering rate of the encrypted data is effectively controlled. However, there is a problem that the information query time is high.

Zhang et al. proposed an anti-peep network security authentication information encryption method [8]. The anti-peep network data attributes are selected according to the professional knowledge and the overall structure of the data, and the selection results are pre-processed. According to the attribute processing result, a variable window is introduced to realize the determination and clearing of redundant data. First, the method sets the minimum, maximum, and minimum thresholds of the variable window and initializes the window. After that, the data to be matched is set, and the segmentation of the string is realized by the 3-gram method. After calculating the similarity between the data to be matched and the window data record, the calculation result is stored in a two-dimensional array. In addition, the data record similarity in the case of missing fields is calculated, thereby realizing the redundancy of each type of data in the network, and then the redundant data in the determination result is cleared. The method treats the plaintext as a continuous bitstream transmitted in the privacy network and inputs its link number into the data encryption. The seed is used to complete the initialization of the key sequence generator and generator, and the random encryption function is called to generate a random encryption number. The encrypted bitstream is then encrypted using the encrypted number. Experiments show that the information anti-attack coefficient is larger after encryption. However, this method has a problem of low resource utilization and cannot effectively meet the needs of users.

Qian et al. proposed a scheme they refer to as Privacy-Preserving Selective Aggregation (PPSA) [9]. PPSA can be described as a method which encrypts users' SPI to prevent privacy disclosure from outside analysts and service providers alike. PPSA fully supports selective aggregate functions that are used for online user-based behavior analysis while also being able to guarantee differential privacy. The authors provided experimental results that show that their model can effectively support both aggregate queries (overall and selective) with acceptable levels of communication and computation overhead. However, due to the fact that some information can be shared, the algorithm has the well-known issues of slow data acquisition speeds.

Zhang et al. proposed a user privacy protection method based on dynamic hiding of sensitive itemsets (SIDH) [10], which senses the positive and negative boundaries of sensitive rules corresponding to the itemsets space and incrementally expands the original snapshot to query anonymous set data. This methodology hides and purifies sensitive association rules dynamically and finally realizes user privacy protection. The experimental results showed that the SIDH method is hidden. The speed of hiding sensitive itemsets is high, but the recognition rate of data is low.

Zhu proposed a new encryption method for privacy information acquisition process [11]. Privacy information in mobile Internet can be divided into several subspaces according to its attributes and acquisition time. Private information is encrypted in each subspace and transmitted to relay nodes. When a given relay node needs to read private information, it needs to request the corresponding sub-key of the private information from data source node. A data source node's own unique strategy decides whether to authorize or not, and ensures the security of all the sub-keys it generates. After encryption, the lengthy private information is divided into smaller information slices by segmentation and reorganization. After transformation, the information is fused to ensure the integrity of the encrypted information. The experimental results showed that the proposed method improves the security and integrity of privacy information acquisition process, but it has issues with long query delay times.

To solve the above problems, an SPI security encryption algorithm based on incremental update data is proposed. Before encrypting data, our algorithm analyzes user data resources and encrypts the data according to the analysis results gauging the type of data involved, as summarized in Section 3.1. This effectively solves the problem of data query delays caused by traditional methods in encrypting large amounts of data by only encrypting data that needs enhanced security and privacy. To solve the problem of low data recognition rate and effective utilization of resources, an interference quantification method is used (described in Section 3.3) to determine the location of specific data after the data are encrypted. The experimental results show that the proposed algorithm effectively solves the shortcomings of traditional methods, and can protect a users' privacy and information security. We also include some discussion of the potential applications of our work. Our work here to our knowledge is both novel in implementation and also in results.

3. Secure Encryption Algorithm for SPI

With the application and development of network physical systems and more specifically CPS, the security of user's trade secrets and private data has gradually become a research hotspot in this field. At present, the application of information technology (IT) in the security architecture of network physical system is not perfect, and the security encryption process of sensitive private message information has problems such as slow information acquisition speed and low recognition rate. Therefore, this paper designs a new SPI efficient encryption algorithm to alleviate such problems. The method first analyzes public data resources, private data resources and mixed data resources in user data. From this analysis, it is concluded which resources need to be encrypted and which data can be shared openly un-encrypted. The key concept here is that not all data fall under the context of SPI, therefore there is no need to waste computational resources to encrypt/decrypt them. The analysis of the data aids in establishing a targeted user data subset for sharing and the encryption structure. User data resources are collected in using an adaptive data collection method. Finally, the data encryption method based on interference quantization is used to complete the analysis on the secure encryption method for SPI. An overview flow chart is given in Figure 1.

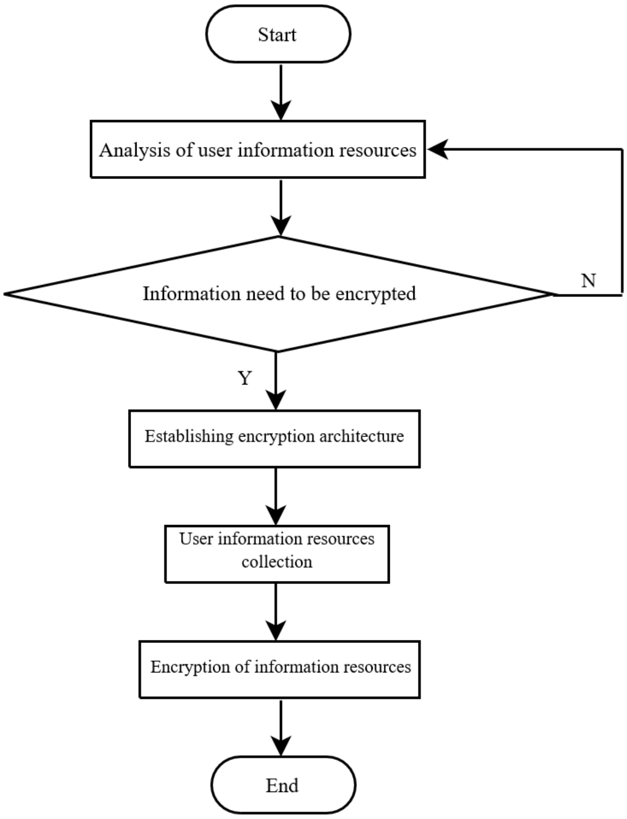
Start
Analysis of user information resources
Information need to be encrypted
N
Y
Establishing encryption architecture
User information resources collection
Encryption of information resources
End

Figure 1. Secure encryption algorithm flow chart.

3.1. SPI Analysis

In the context of incremental data updates, SPI is mainly classified into three types: public data resources, private data resources, and mixed data resources, depending on the scope and type of information.

1. **Public data resources**

   Public data resources refer to users' information stored on servers not under their direct control, which can be accessed by other users through open channels and can be understood without users having strong professional knowledge. The cost of public data acquisition is relatively low, and it is a relatively low level of privacy security category [12]. Some common data and Web data information belong to public data, including personal credit information, e-mail addresses, browsing traffic, job categories and other similar information. This kind of data resources is mainly used by users themselves and others, and will not usually threaten users' privacy. Users do not need to worry about the source of resources and data security, but only pay attention to the satisfaction of information and the utilization of attached resources.

2. **Private data resources**

   Private data resources exist in the users' own storage system, mainly for information that cannot be publicly obtained, involving SPI and potentially some relatively important business data and other non-public private data, which can be divided into personal account login account and password, user identity card information, electronic financial information, and individuals/business data, among others [13]. Private data need a high level of privacy and security. They cannot be acquired and utilized by people other than public administration departments. At the same time, external organizations cannot access this part of any resources.

3. **Mixed data resources**

   Mixed data resources are the collection of public data resources and private data resources. Through the network, data security can be balanced between public data resources and private data resources [14]. User's private data resources are linked with public data resources to form a user's mixed data resources. Specifically, it includes the personal account login account and password, user ID card information and personal credit information, mailbox address and other information in public information.

Private data resources belong to the privacy information of individual users, and cannot be obtained and used by people other than public administration departments. Therefore, this paper mainly encrypts private data resources. The natural combination of different systems and distributed resources can realize the secure encryption of data resources. The user privacy information resource structure is represented by Figure 2.

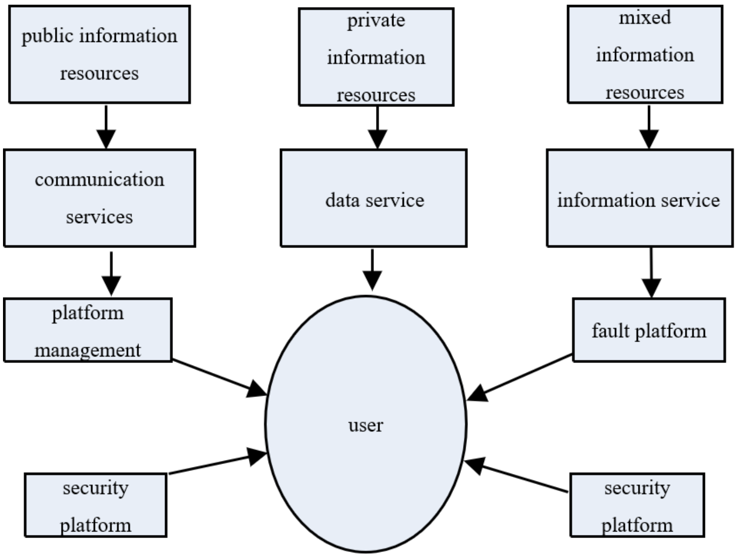

Figure 2. SPI resource structural map.

3.2. SPI Collection

Combined with the above definitions of SPI resources, the adaptive data collection method is used to collect SPI. After instructions are sent to specify the tasks for data collection, appropriate data collection tasks and a decision module are selected to meet the needs of the tasks. Concurrently, privacy information is gathered by the data processing module to integrate the resources [15,16].

For collection, suppose there are q parameter collection tasks for completing of data collection. The goal of data collection is to make a reasonable assignment of the q tasks.

Suppose a parameter detection task Q occurs at a certain moment of time. An alliance is introduced, and the task assignment is performed in the area where the collection task appears. According to the different requirements of acquisition task Q_m, the task is decomposed into $Q_m = \{Q_{m1}, Q_{m2}, \cdots, Q_{mi}\}$. The appropriate data acquisition is selected to form the corresponding data alliance A_m, $A_m = \{P_{m1}, P_{m2}, \cdots P_{mi}\}$. The acquisition task is assigned in the data alliance, P_{mi} carries on the sub-task Q_{mx} of the acquisition task, $Q_{mx} \in Q_m, (x = 1, 2, \cdots, i)$, and the results are transmitted to the electronic storage library.

To achieve efficient and real-time detection of the user privacy data parameters, and effectively improve the performance of data resources, the time of data collection is used as an evaluation function. The time of data acquisition can be represented by a matrix of $q \times q$, where the information element ext_{mn} represents the execution time of acquisition task m at the information node P_n.

The execution time of acquisition task mainly includes: the time of data transmission ext_{mn}^{tr}, the overhead time ext_{mn}^{oh} and the time spent on data processing ext_{mn}^{pr}:

$$ext_{mn} = ext_{mn}^{tr} + ext_{mn}^{oh} + ext_{mn}^{pr} \tag{1}$$

The total amount of data resources is related to transmission time ext_{mn}^{tr} and amount of data D_{tr}, $ext_{mn}^{tr} = D_{tr}$. Overhead time ext_{mn}^{oh} depends on the packet size. Assuming that the writing time and reading time of a packet is equal, the relationship between overhead time, data visits D_{oh} and data resource storage speed V can be expressed as: $ext_{mn}^{oh} = 2D_{oh}/V$. Data processing time ext_{mn}^{pr} is different because of different tasks.

$r\left(P_m\right)$ represents the sum of time of node P when performing the information acquisition task Q_m, and $t\left(Q_m\right)$ represents the sum of time when data resource acquisition task performs q tasks, which can be represented as:

$$\begin{aligned} t\left(P_m\right) &= \sum_{n=1}^{p} ext_{mn} \\ t\left(Q_m\right) &= \sum_{m=1}^{q} t\left(P_m\right) \end{aligned} \tag{2}$$

The energy consumption of data nodes includes energy consumption of computing data resources C_{pro}, and energy consumption of communication data C_{com}.

The energy consumption of computing data resources is the energy consumption of processing tasks for data acquisition. If $S\left(P_n\right)$ is the energy consumption of tasks perfumed by P_n in time, and energy consumption of computing when data node P_n processes task can be expressed as:

$$C_{pro}\left(P_n\right) = \sum_{m=1}^{q} S\left(P_n\right) ext_{mn} \tag{3}$$

The data energy consumption is generated during the process of data transmission. The energy consumption of data transmission is $C_{0,com}$ at a given distance of d_0, and the data energy consumption is related to spatial distance d_{in} between central data nodes P_i and P_n:

$$C_{i,com} = \frac{d_{in}^2}{d_0^2} \times \frac{(4\pi)^2 \beta}{G_t G_r \lambda^2} \times C_{0,com} \tag{4}$$

In Equation (4), G_t represents the emission coefficient of data node P_i, G_r is the receiving coefficient of data node P_n, λ represents wavelength of communication, β is factor of data power, and all parameters are constant. $(4\pi)^2 \beta / G_t G_r \lambda^2 \times C_{0,com}$ stands for constant. thus, transmission energy consumption of a unit of data can be evaluated with d_{in}^2/d_0^2.

The energy consumption C of data can be expressed as:

$$C = \sum_{n=1}^{P} \left(C_{pro} + C_{com}\right) \tag{5}$$

The data load balance degree represents the difference range of time for performing the acquisition task and time of completing the acquisition. The ratio of difference to data acquisition time [17,18] is used to describe the information load balance degree, which can be defined as:

$$L = 1 - \sum_{m=1}^{q} \left(T - t\left(P_m\right)\right) / \left(q \times T\right) \tag{6}$$

In Equation (6), T indicates the total time to complete the data acquisition, $T = \max_{m=1}^{q} \left(t\left(P_m\right)\right)$.

By the above process, the collection of user privacy information resources has been completed.

3.3. Security Encryption Method of UPI

Combined with the above-mentioned collection techniques of user data, the interference quantization method is used to facilitate the encryption of large amounts of SPI [19].

Assuming k is fixed and represented by (k), the problem of resource encryption in (k) data can be represented as:

$$\begin{cases} \max \sum\limits_{j \in J} \sum\limits_{i \in I} R_{ij}^{(k)} x_{ij}^{(k)} \\ s.t \quad \sum\limits_{i \in I} x_{ij}^{(k)} = 1 \end{cases} \tag{7}$$

In Equation (7), $R_{ij}^{(k)}$ indicates the total amount of SPI, and $x_{ij}^{(k)}$ indicates the amount of mixed data.

By solving Equation (7), X of all k are worked out. We give j as fixed in (j), the resource sharing problem on the (j)th data is considered, and $P_{(j)}^{k} \in [0.P_{\max}]$ is considered separately, it can be derived that:

$$\begin{cases} \max \sum\limits_{k \in K} R_{(j)}^{k} \\ s.t \quad \sum\limits_{k \in K} G_{(j)}^{tk} P_{(j)}^{k} \leq 1_{th} \end{cases} \tag{8}$$

In Equation (8), $R_{(j)}^{k}$ indicates the rate at which data is encrypted. The data objective function $\Sigma_{k \in K} R_{(j)}^{k}$ can be used to sum up k to get:

$$\Sigma_{k \in K} R_{(j)}^{k} = \log_2 \left\{ \frac{\sum\limits_{k \in K} G_{(j)}^{\bar{k}} P_{(j)}^{\bar{k}} + \sum\limits_{t \in T} I_{(j)}^{ht} + n_{(j)}^{k}}{\sum\limits_{\bar{k} \in K/k} G_{(j)}^{k} P_{(j)}^{k} + \sum\limits_{t \in T} I_{(j)}^{ht} + n_{(j)}^{k}} \right. \tag{9}$$

In Equation (9), $I_{(j)}^{ht}$ indicates the interference item after encryption of SPI is determined. We have seen that conventional data encryption usually needs to solve complex non-convex optimization problems as given in [20]. However, here, we use interference encryption to simplify the problem. For ease of description, some auxiliary variables are introduced. $v_{(j)}^{th}$ represents the interference of k resources on the jth SPI resource, and the formula given in Equation (8) is converted into Equation (10), which is called the SPI interference problem.

$$\begin{cases} \max \sum\limits_{k \in K} R_{(j)}^{k} \\ s.t \quad \sum\limits_{k \in K} v_{(j)}^{tk} \leq I_{th} \end{cases} \tag{10}$$

In Equation (9), $P_{(j)}^{\bar{k}} = v_{(j)}^{tk} / G_{(j)}^{\bar{k}}$, $P_{(j)}^{k}$ is a function of $v_{(j)}^{tk}$, and the data variable is $P_{(j)}^{k} = v_{(j)}^{tk} \in \left[0, G_{(j)}^{tk} P_{\max}\right]$. It is worth noting here that the constraint of interference becomes a form of summation of simple variables. Thus, the SPI encryption method of interference quantization can be introduced to simplify the original data encryption interference problem [21–26].

Dealing with individual user data: assuming that Δv represents the infinitesimal of interference, it can only be shared as a region, and the length of the quantization is L, thus $I_{th} = L \Delta v$. Equation (10) can be simplified into L, and the infinitesimal Δv of interference can be divided into the largest objective function [27–30]. Let $l \in \{1.2. \cdots, L\}$ indicate step l, and Δv^{l} represents the interference infinitesimal of step l, and when information is single, the information interference infinitesimal of each step is equal.

$$\Delta v^{l} = \Delta v = I_{th} / L \tag{11}$$

In Equation (11), when Δv^{l} shares with the kth data, the corresponding resource infinitesimal is given by Equation (12):

$$\Delta P^k_{(j)} = \frac{\Delta v^l}{G^{tk}_{(j)}}, \forall k \in K \tag{12}$$

Dealing with multiple resources of data, suppose that, by L step, the interfering micro-components are distributed to massive data, then:

$$\Delta v^l = \frac{I_R}{L+1-l} \tag{13}$$

In Equation (13), I_R represents remaining interference quantification of data, and is updated according to Equation (14):

$$I_R = I_{th} - \sum_{k\in K} G^{tk}_{(j)} P^k_j \tag{14}$$

In Equation (14), the data vector $P_{(j)}$ is updated at each step according to the SPI to interfere with the resources corresponding to the micro-cloud. Considering that multiple resources of data are disturbed, when Δv^l share the kth data, the corresponding resource infinitesimal takes the minimum value of data, and Equation (15) is given:

$$\Delta P^k_{(j)} = \min\left\{\frac{\Delta v^l}{G^{tk}_{(j)}}\right\}, \forall \in K \tag{15}$$

By the above conversion, this paper can simplify the encryption of interference data of SPI. $F_{(j)}\left(\Delta v^l, k\right)$ represents the function goals in Equation (9) when Δv^l shares to kth data. At each step, the maximum data $F_{(j)}\left(\Delta v^l, k\right)$ brought by π^l is numbered as (π^l), which can be expressed as:

$$\pi^l = \arg\max\left\{F_{(j)}\left(\Delta v^l, k\right)\right\} \tag{16}$$

Finally, the SPI resource encryption vector $P_{(j)}$ is obtained. The privacy of the data is completed and can be updated as securely encrypted. Algorithm 1 is obtained from summarizing the Encryption process using Equations (1)–(16). We also expand Algorithm 1 by showing the Key Expansion Function in Algorithm 2.

Algorithm 1: Encryption algorithm.

```
Procedure Dec-MDP($ext^{pr}_{mn}$, $ext^{tr}_{mn}$, $ext^{oh}_{mn}$, $t_{pm}$, $t_{qm}$, $C_{pro}$, $C$, $L$, $K$, $ext_{mn}$)
//Single task consumes time $ext^{tr}_{mn}$, $ext^{oh}_{mn}$
//Total consumption time tpm, $t_{qm}$;
//Energy Consumption for Single Task $C_{pro}$
//Task Total Energy Consumption $C$
//Load Balancing Parameters $L$
//Constraint parameter $K$
//Total Time-consuming Constraint Variables $ext_{mn}$
$d_0 \leftarrow$ Fixed distance
$d_{in} \leftarrow \sqrt{P_i - P_n}$
$G_t \leftarrow P_i$
$G_r \leftarrow P_n$
$C \leftarrow \frac{d^2_{in}}{d^2_0} \times \frac{(4\pi)^2 \beta}{G_t G_r \lambda^2} \times C_0$;
$m \leftarrow 1$
```

```
while $m < q$ do
    T-t(p$_m$);
    $Sum \leftarrow Sum + T - t(p_m)$;
    m+1
$L \leftarrow 1 - Sum/\ (q \times T)$;
$ext_{mn} \leftarrow ext^{tr}_{mn} + ext^{oh}_{mn} + ext^{pr}_{mn}$;
while $m < q$ do
    $Sum_2 \leftarrow Sum_2 + t(p_m)$;
    $m+1$
$t_{\mathrm{qm}} \leftarrow Sum_2$;
while $n < p$ do
    Sum$_3$←Sum$_3$+ext$_{mn}$;
    n+1
$t_{\mathrm{pm}} \leftarrow Sum_3$
if $(ext_{mn} < ConstraintvalueandC < ConstraintvalueandL < Constraintvalue)$; then
    //Represents an interference-free encryption process
    KeyExpansion(byte key{4*RK}),word w{GK*(PK+1),RK}
    begin
        Word temp
        i=0
        while (i<RK) do
            W{i}=word(key[4*i],key[4*i],key[4*i],key[4*i])
            i=i+1
        i=GK
        while (i<GK*(PK+1)) do
            Temp=w[i-1]
            if (i mod RK==0) then
                Temp=SubWord(Max(temp))xor Rcon[i/RK]
            else
                Temp=SubWord(temp)
            w[i]=w[i-RK] xor temp
            i=i+1
    //Implement encryption
//Interference exists
$\Delta v^l \leftarrow \frac{I_R}{L+1-l}$; //Optimization parameters
while $k < K$ do
    Sum$_4$ ←Sum$_4$ + $G^{tk}_{(j)} P^k_j$;
    k+1
$I_R \leftarrow I_{th} - Sum_4$
while $k < K$ do
    If $\frac{\Delta v^l}{G^{tk}_{(j)}} > \frac{\Delta v^l}{G^{tk+1}_{(j)}}$
    min← $\frac{\Delta v^l}{G^{tk+1}_{(j)}}$;
    k+1
$\Delta P^k_{(j)} \leftarrow$ min; //Iterative updating
```

Algorithm 2: Key expansion function.

```
Procedure KeyExpansion(byte key{4*$R^K$}), word w{GK*($P^K$+1),$R^K$}
begin
    Word temp
    i=0
    while ($i<R^K$) do
        W{i}=word(key[4*i],key[4*i],key[4*i],key[4*i])
        i=i+1
    end
    i=$G^K$
    while ($i<G^K*(P^K+1)$) do
        Temp=w[i-1]
        if ($i$ mod $R^K$==0) then
            Temp=SubWord(Max(temp))xor Rcon[i/$R^K$]
        else
            Temp=SubWord(temp)
        end
        w[i]=w[i-$R^K$] xor temp
        i=i+1
    end
    //Implement encryption
end
```

4. Experimental Results and Analysis

4.1. Experimental Setup

We selected the data provided by Google Dataset Search dataset as the experimental data source [31].

Google Dataset Search dataset can be regarded as a one-stop dataset shop, which contains massive data of different sizes and types from sources such as NASA and ProPublica. The data source is comprehensive, so the dataset has strong applicable value. Through `MATLAB 8.0` software, a large-scale data resource experimental platform for interference quantification was built, and used for data processing. Taking data acquisition time, information resource recognition rate, information query delay and effective utilization of resources as experimental indicators, the proposed method was compared with those peers from [6–9] to verify the effectiveness of our method. All methods from [6–9] were rerun and compared with our method. All models were implemented in the Matlab R2017b software environment and has been subject to processing and analysis as described next.

4.2. Analysis of Experimental Results

Figure 3 shows the comparison of data acquisition speeds of the proposed method with the peer methods in [6–9]. In the cases with the same amount of data, we observed a shorter acquisition time coupled with higher efficiency of data acquisition. Therefore, we used data collection time to verify the collection efficiency. The specific results are shown in Figure 3. One item of note here is that, as the information resources increase, most other methods show a linear increase in collection time, whereas our method shows more of a constant relationship staying consistent throughout increase in information.

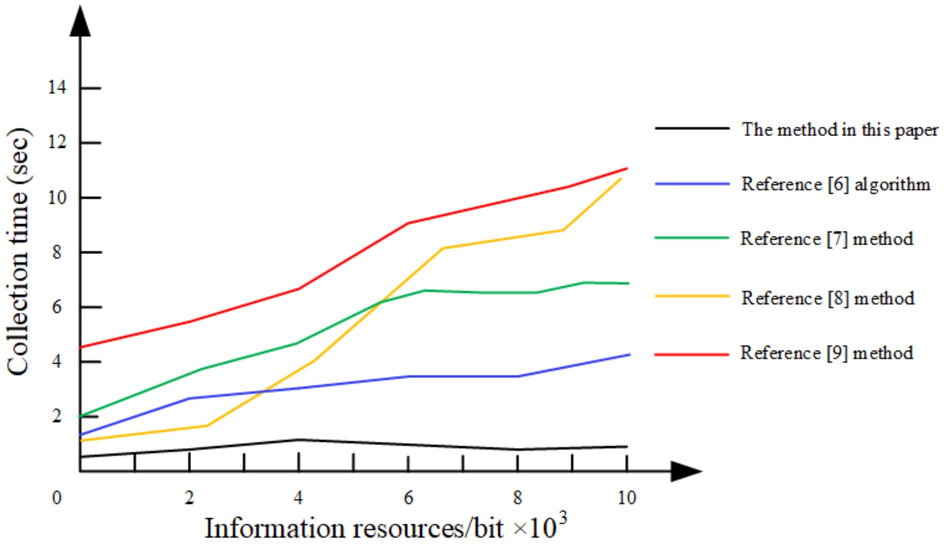

Figure 3. SPI collection time.

Analysis of Figure 3 shows that the private data collection time of the five methods is different. The acquisition time of the methods in [6] is between 1.4 s and 4.2 s, and the acquisition time of the method given in [7] is between 2.1 s and 6.7 s. The acquisition time of the method given in [8] is between 1.2 s and 10.8 s, and the collection time of private information is relatively long. The acquisition time of the methods [9] is between 4.5 s and 10.8 s. We attribute these valid data to the algorithm using an adaptive data collection method, which enables the decision module while the data collection task is being performed, saving a lot of time and meeting the task requirements.

To verify data recognition accuracy of the methods, we again used algorithms from [6–9] to compare to our algorithm under different data resource scenarios. The results are shown in Figure 4.

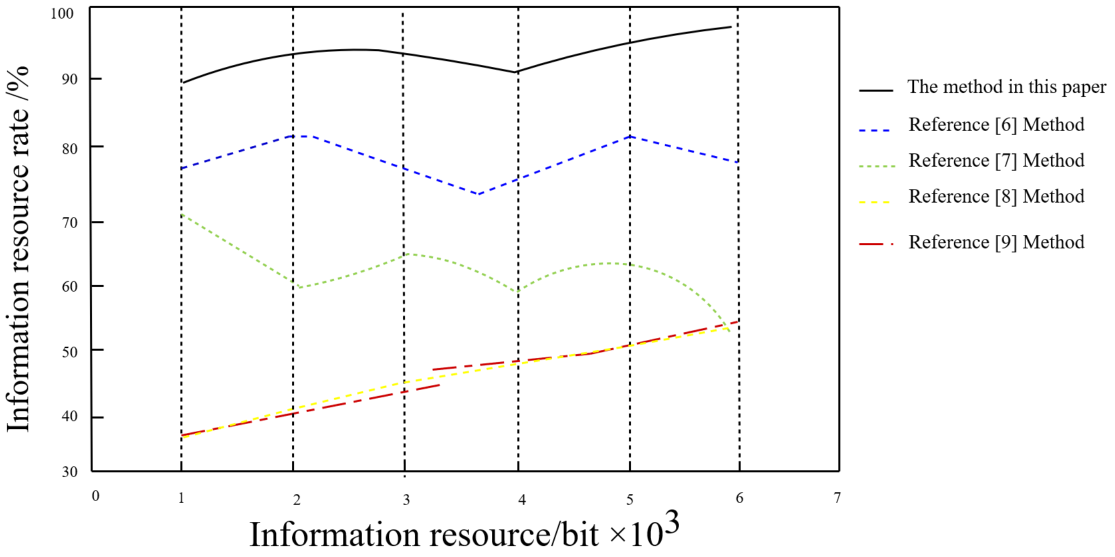

Figure 4. Recognition rate of information resources.

The analysis of Figure 4 shows that, when the resource quantity is 1 × 10^3 bit, the data recognition rates of the methods [6–9] are 69%, 78%, 37%, and 36%, respectively. The data recognition rate of our algorithm is 92%. When the resource quantity is 6 × 10^3 bit, the data recognition rates of the methods from [6–9] are 59%, 80%, 62%, and 64%, respectively. Comparatively, data recognition rate of our algorithm is slightly over 90%. Observing the overall graph in Figure 4, the data recognition rate of the algorithm is always best, indicating our algorithm has a high data recognition rate and good recognition performance [32]. We attribute this to the fact that conventional information encryption needs to solve complex non-convex optimization problems. However, our method simplifies the problem in a different way, known as interference encryption. To make the description more convenient, some auxiliary variables are introduced, which reduce the influence of interference items and improves the recognition rate of effective data. One unexplained behavior to note is the decrease in rate where the information resource quantity is 4 × 10^3 bit; however, after this amount, as expected, this is a slight increase. This unexplained decrease may be attributed to some special behavior of the algorithm at that amount of data.

Figure 5 shows the comparison of delay caused by data resource queries in seconds of our proposed algorithm with delays in [6–9].

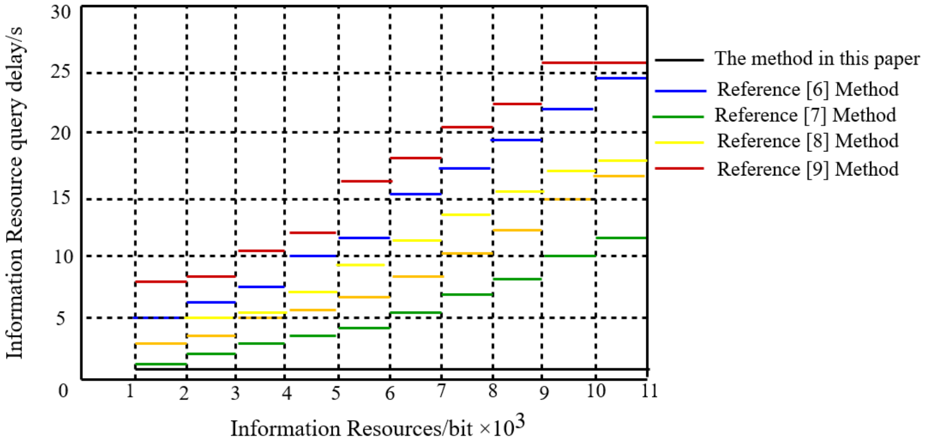

Figure 5. Privacy information query latency.

Analysis of Figure 5 shows that the query delay of the five methods increases as the amount of data resources are increased. When the private data used in the query are 6 × 10^3 bit, the `SPI` query delays of [6–9] are 10.5 s, 8.5 s, 5.5 s, and 18 s, respectively. Similarly, our algorithm creates a delay of just above 1 s. When the amount of private data used in the query reach 10 × 10^3bit, the privacy data query delays from [6–9] are 24.5 s, 16.5 s, 11.5 s, and 26 s, respectively. In comparison, our algorithm creates a delay which is still approximately 1 s. A user would not notice a change in delay even if the private data used in a query were increased. This clearly indicates that the data resource query delay of our algorithm is small, has better query performance, and is more feasible for large data storage applications. Our algorithm over the whole set of information resource amounts performed better than all comparable reference methods.

Table 1 shows the comparison of the utilization rate of information resources (%) between the methods from [6–9] and our algorithm.

Table 1. Comparison of utilization rates of information resources of the proposed method with peers.

Privacy Information	**Methods**				
(×10^3 bit)	**Reference [6]**	**Reference [7]**	**Reference [8]**	**Reference [9]**	**Method (ours)**
10	69	78	68	85	90
15	63	82	74	76	92
20	65	78	73	81	95
25	68	82	67	73	93
30	62	80	72	80	97

Analysis of Table 1 shows that the utilization of data resources of the four methods is different in the case of different amounts of private data. When the private data are 10 × 10^3 bit, the resource utilization rates of from [6–9] are 69%, 78%, 68%, and 85%, respectively. In comparison, the resource utilization rate of our proposed algorithm is 90%. When the private data are 30 × 10^3 bit, the resource utilization rates from [6–9] are 62%, 80%, and 72%, and 80%, respectively. Comparatively, the resource utilization rate of our algorithm is 97%. It can be seen in Table 1 that, regardless of the amount of private data, the resource utilization rate of our algorithm exceeds 90%, and from this it can be concluded that the resource utilization is strong.

Based on the above experimental results, our algorithm can effectively improve the collection time of private data, increase the recognition rate of data resources, lessen the delay caused from queries of private data, and increase the utilization of data resources. As a result, we can conclude that our encryption algorithm exceeds some of the current algorithms from [6–9] in overall performance.

5. Conclusions

With the rapid development of the Internet, information dissemination is oriented to the needs of users. According to practice, in the society of information proliferation and resource reorganization, secure encryption of private information is a requirement for all data. In privacy encryption process of private data, the existing methods cannot effectively enhance the security of information, and cannot meet the different needs of users based on specific usage tendencies. To this end, a private data security encryption algorithm for incremental update data is proposed to protect `SPI`. The experimental results clearly show that the resource utilization rate of this algorithm is 97%, which is much higher than that of the traditional methods. Moreover, data acquisition time of our algorithm is less than 1.0 s, which is much lower than that of the traditional methods as well. This is due to the fact that the algorithm in this paper adopts the adaptive data collection method, enabling the decision module while the data collection task is going on, which saves a lot of time and meets the requirements of the task. This shows that our algorithm has better encryption effects and can effectively improve the security of information. Compared to traditional methods, we show that data resource recognition rate and utilization rates are higher and that data query delay is lower, which is because our algorithm simplifies the problem in different ways, called interference encryption. It introduces some auxiliary variables, which reduces the influence of interference items and improves the effective data, showing the effectiveness of our proposed methodology. This in turn indicates that the algorithm can effectively solve the shortcomings of traditional methods and has practical application.

Author Contributions: Conceptualization, G.S. and X.Z.; methodology, G.S.; validation, X.Z. and R.M.P.; formal analysis, X.Z.; writing—original draft preparation, X.Z.; writing—review and editing, G.S.; project administration, and R.M.P.

Funding: The APC was funded by MDPI.

Acknowledgments: The authors would like to thank Dr. Shuai Liu, Hunan Normal University for his support with this publication.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zhang, C.; Wang, B.; Li, W.; Huang, S.; Kong, L.; Li, Z.; Li, L. Conversion of invisible metal-organic frameworks to luminescent perovskite nanocrystals for confidential information encryption and decryption. *Nat. Commun.* **2017**, *8*, 1138. [CrossRef] [PubMed]
2. Wang, X.; Li, W.; Li, W.; Gu, C.; Zheng, H.; Wang, Y.; Zhang, S.X.A. An RGB color-tunable turn-on electrofluorochromic device and its potential for information encryption. *Chem. Commun.* **2017**, *53*, 11209–11212. [CrossRef] [PubMed]
3. Xiao, D.; Li, X.; Liu, S.J.; Wang, Q.H. Encryption and display of multiple-image information using computer-generated holography with modified GS iterative algorithm. *Opt. Commun.* **2018**, *410*, 488–495. [CrossRef]
4. Lu, Y.; Zhu, M. Privacy preserving distributed optimization using homomorphic encryption. *Automatica* **2018**, *96*, 314–325. [CrossRef]

5. Poh, G.S.; Chin, J.J.; Yau, W.C.; Choo, K.K.R.; Mohamad, M.S. Searchable symmetric encryption: Designs and challenges. *ACM Comput. Surv. (CSUR)* **2017**, *50*, 40. [CrossRef]
6. Zhang, C.L.; Xiong, L.; Lu, L.C. Simulation of Double-Encrypted Reversible Concealment Algorithm for Real-time Network Information. *Comput. Simul.* **2018**, *35*, 201–204+268. (In Chinese)
7. Solomon, M.; Elias, E.P. Privacy Protection for Wireless Medical Sensor Data. *Int. J. Sci. Res. Sci. Technol.* **2018**, *4*, 1439–1440.
8. Zhang, K.; Douros, K.; Li, H.; Li, H.; Wei, Y. Systems and methods for pressure-based authentication of an input on a touch screen. U.S. Patent 8,988,191, 24 March 2015.
9. Qian, J.; Qiu, F.; Wu, F. Privacy-Preserving Selective Aggregation of Online User Behavior Data. *IEEE Trans. Comput.* **2016**, *66*, 326–338. [CrossRef]
10. Zhang, H.T.; Zhu, Y.H.; Huo, X.Y. User privacy protection method based on dynamic hiding of sensitive items. *Appl. Res. Comput.* **2017**, *34*, 3740–3744.
11. Zhu, L.N. Research on Encryption Simulation of Private Information Acquisition Process over Mobile Internet. *Comput. Simul.* **2018**, *8*, 156–159.
12. Chen, Y.R.; Rezapour, A.; Tzeng, W.G. Privacy-preserving ridge regression on distributed data. *Inf. Sci.* **2018**, *451*, 34–49. [CrossRef]
13. Grice, W.P.; Evans, P.G.; Lawrie, B.; Legre, M.; Lougovski, P.; Ray, W.; Williams, B.P.; Qi, B.; Smith, A.M. Two-party secret key distribution via a modified quantum secret sharing protocol. *Opt. Express* **2015**, *23*, 7300–7311. [CrossRef] [PubMed]
14. Quan, L.-X. Storage Method and Implementation of Education Resource Ontology in a Relational Database. *J. Langfang Teach. Univ. (Nat. Sci. Ed.)* **2016**, *2*, 3.
15. Liu, S.; Pan, Z.; Cheng, X. A Novel Fast Fractal Image Compression Method based on Distance Clustering in High Dimensional Sphere Surface. *Fractals* **2017**, *25*, 1740004. [CrossRef]
16. Dou, Y.; Chan, H.C.; Au, M.H. A Distributed Trust Evaluation Protocol with Privacy Protection for Intercloud. *IEEE Trans. Paral. Distrib. Syst.* **2018**, *30*, 1208–1221. [CrossRef]
17. Luo, Z.Y.; Shi, R.H.; Xu, M.; Zhang, S. A novel quantum solution to privacy-preserving nearest neighbor query in location-based services. *Int. J. Theor. Phys.* **2018**, *57*, 1049–1059. [CrossRef]
18. Wang, L.; Zhang, Z.; Dong, M.; Wang, L.; Cao, Z.; Yang, Y. Securing Named Data Networking: Attribute-Based Encryption and Beyond. *IEEE Commun. Mag.* **2018**, *56*, 76–81. [CrossRef]
19. Aminifar, A.; Eles, P.; Peng, Z. Optimization of Message Encryption for Real-Time Applications in Embedded Systems. *IEEE Trans. Comput.* **2017**, *67*, 748–754. [CrossRef]
20. Gao, C.Z.; Cheng, Q.; He, P.; Susilo, W.; Li, J. Privacy-preserving Naive Bayes classifiers secure against the substitution-then-comparison attack. *Inf. Sci.* **2018**, *444*, 72–88. [CrossRef]
21. Xia, Y.; Chen, W.; Liu, X.; Zhang, L.; Li, X.; Xiang, Y. Adaptive multimedia data forwarding for privacy preservation in vehicular ad-hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2629–2641. [CrossRef]
22. Dwivedi, A.D.; Morawiecki, P.; Srivastava, G. Differential cryptanalysis of round-reduced speck suitable for internet of things devices. *IEEE Access* **2019**, *7*, 16476–16486. [CrossRef]
23. Bryce, R.; Shaw, T.; Srivastava, G. Mqtt-g: A publish/subscribe protocol with geolocation. In Proceedings of the 2018 41st International Conference on Telecommunications and Signal Processing (TSP), Athens, Greece, 4–6 July 2018; pp. 1–4.
24. Dwivedi, A.D.; Dhar, S.; Srivastava, G.; Singh, R. Cryptanalysis of Round-Reduced Fantomas, Robin and iSCREAM. *Cryptography* **2019**, *3*, 4. [CrossRef]
25. Srivastava, G.; Fisher, A.; Bryce, R.; Crichigno, J. Green Communication Protocol with Geolocation. In Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; pp. 1–6.
26. Malina, L.; Srivastava, G.; Dzurenda, P.; Hajny, J.; Fujdiak, R. A Secure Publish/Subscribe Protocol for Internet of Things. In Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019.
27. Yao, Z.; Ge, J.; Wu, Y.; Jian, L. A privacy preserved and credible network protocol. *J. Parallel Distrib. Comput.* **2019**, *132*, 150–159. [CrossRef]
28. Ma, Y.; Wu, Y.; Li, J.; Ge, J. APCN: A Scalable Architecture for Balancing Accountability and Privacy in Large-scale Content-based Networks. *Inf. Sci.* **2019**, *484*, 27–43. [CrossRef]

29. Zhou, R.; Zhang, X.; Wang, X.; Yang, G.; Wang, H.; Wu, Y. Privacy-preserving data search with fine-grained dynamic search right management in fog-assisted Internet of Things. *Inf. Sci.* **2019**, *491*, 251–264. [CrossRef]
30. Tian, Y.; Guo, J.; Wu, Y.; Lin, H. Towards Attack and Defense Views of Rational Delegation of Computation. *IEEE Access* **2019**, *7*, 44037–44049. [CrossRef]
31. Google Search Datasets. Available online: https://developers.google.com/search/docs/data-types/dataset (accessed on 11 September 2019).
32. Sakhnini, J.; Karimipour, H.; Dehghantanha, A.; Parizi, R.M.; Srivastava, G. Security Aspects of Internet of Things aided Smart Grids: A Bibliometric Survey. *Internet Things* **2019**, 100111. [CrossRef]