Algorithmic Analysis on Adaptive Dragonfly based Optimal Key Generation for Privacy Preservation in IoT

Ravindra S. Apare, Satish N. Gujar

Abstract: ***The Internet of Things (IoT) is a network of Internet-enabled devices that can sense, communicate, and react to changes in their environment. It is commonly applied in many applications, like building automation, medical healthcare systems, transportation, environment monitoring, and energy management. Billions of these computing devices are connected to the Internet to exchange data between themselves and/or their infrastructure. However, the privacy of data seems to be the greatest issue that needs to be solved. This paper intends to develop an improved data sanitization and restoration framework in IoT for higher-order privacy preservation. The preservation process is carried out using key that is optimally selected. For the optimal selection of key, a new Improved Dragonfly Algorithm (IDA) is introduced. Finally, the algorithmic analysis is carried out by varying parameters like enemy distraction weight*** (e) ***and food attraction weight*** (f) ***of the proposed algorithm.***

Keywords: IoT; Privacy Preservation; Data Sanitization; Data Hiding; key Generation; IDA.

I. INTRODUCTION

Over the decades in the era of connected devices, an incredible revolution is marked by IoT in every aspect of human life. Since human life is becoming more dependent on smart devices, the necessity of interconnection between the smart devices (IoT devices are generally defined as smart devices) are uprising and resulting in wider generation of data [9] [10]. The data being generated each day are in the unconditional and unstructured format. In the universe of IoT, every entity in the real world is virtual, which means every person and thing becomes addressable with a unique IP, locatable and at the same time readable. IoT is a network of the internet-enabled devices that has the potential of sensing, communicating and reacting to the dynamic changes in the environment [8] [11].

IoT do not have a centralized agency to cope up with the issues curtailing in the network and hence essential steps are to be taken in authenticating the server. Since the smart devices have constrained memory and battery storage, they are to be served with lower cost, weightless and higher performance solutions in terms of privacy [6] [7]. On the

other hand, in the IoT environment, there is no prior knowledge about the others and so the detection of the intruder is a big challenge.

Since IoT has penetrated in every nook of the human life from transport to health and entertainment to interact with government, the count of the sensitive data is increasing and at the same time the count of attackers is also growing [16] [17]. Further, to avert the sensitive data from unauthorized access and to resist the equipment from attacks, it is utmost vital for IoT practitioners to design secure and privacy preserved IoT systems with appropriate architectural approach [12] [13].

A huge count of researchers has been undergone in privacy preservation in IoT. Among them, the Cryptographic techniques are the most dominant one as it has the ability to overcome the obstacles in sensitive data preservation. But, this technique has only a limited count of resources and inadequate security protocols. In addition to the encryption and awareness on privacy, one viable solution to secure the privacy of data is access control [14] [15]. It has the potential of taking fine-grained authorization decisions and giving the users an opportunity to manage their own data. Apart from these advantages, it isn't able to overcome the obstacles of protecting the privacy of confidential data [18] [19] [20]. Further, most of the researchers arrived in IoT privacy hasn't focused well on privacy preservation, such that some degree of efforts needs to be introduced with the help of the optimization concepts.

The major contribution of this research work is described below:

- Improved data sanitization and restoration framework is constructed in IoT with the intention of achieving higher-order privacy preservation.
- The key selection plays a major role here and so with the optimally selected key, the data preservation process is carried out.
- As a novelty, for the optimal selection of key, a new IDA is introduced and it is the improved version of the existing DA.
- Finally, the algorithmic analysis is carried out by varying parameters like enemy distraction weight (e) and food attraction weight (f) of proposed IDA.

The leftover section of this paper is organized as: Section II portrays about the literature works undergone in privacy preservation in IoT. Then, proposed data privacy preservation: architecture and objective function is described in Section III. The proposed improved dragonfly for optimal key generation is portrayed in Section IV and Section V tells about the data hiding and data restoration: architectural description. The results acquired from the analysis are discussed in Section VI. Section V concludes the paper.

Revised Manuscript Received on April 25, 2020.

Ravindra S. Apare*, JJT Research Scholar, JJT University, Jhunjhunu, Rajasthan, India .
Satish N. Gujar, Professor, BSCOE&R, Narhe, Pune, Maharashtra

II. LITERATURE REVIEW

A. Related works

In 2019, Guan *et al*. have developed APPA: a device-oriented Anonymous Privacy-Preserving scheme with Authentication in fog-enhanced IoT systems with the intention of performing data aggregation applications [1]. The authors had introduced the proposed model to support SD as well as FN local management (multi-authority). They have recognized the anonymity of SDs by means of deploying pseudonym certificates. Further, with the aid of the security analysis as well as evaluation in performance, the authors have demonstrated both the efficiency as well as the security of APPA scheme.

In 2019, Sharma *et al*. have designed a novel solution with edge-crowd integration in the form of fission computing for trust preservation and also to preserve the rules in Social-Internet of Things (S-IoT) [2]. In the proposed model, the authors had maintained the trust of S-IoT by means of modeling the entropy and had deployed the crowd sources as mini-edge servers. Further, with the aid of numerical simulations, they have evaluated the privacy of S-IoT by cooperative trust relaying (CTR) and privacy-preserving solution.

In 2019, Anatoly *et al*. have proposed CHPC (Cultural Heritage Preservation and Conservation) approach for smart museum systems on the basis of IoT, Artificial Intelligence (AI) and Semantic Web technologies [3]. This approach was developed with the intention of controlling as well as regulating the parameters automatically in the exhibition halls. The proposed model has four layers, namely data collecting layer, light-weight analysis and estimation layer, data management and processing layer and regulating layer. In addition, the authors have introduced the Device Identification service that aid in identifying the devices and when a new device gets connected micro-service ensures the privacy of the existing devices by providing a notification. In case of an authorized device, the authentication process is neglected and the proposed model thus was appropriate to privacy preservation.

In 2018, Wang *et al.* have developed a privacy-preserving raw data collection scheme (PPRD-CS) for IoT with the intention of securing the privacy of the data [4]. Here, the authors have collected the participants data and have obfuscated the collected data over the data of the other participants in the group with the intention of masking the privacy of the individual. The authors haven't gained the help of the trusted authority (TA) and even have made the system adequate for real- world application.

In 2018, Gheisari *et al.* have developed an IoT-based smart city with Software Defined Networking paradigm [5]. Their aim was based on leveraging the benefits of Software Defined Networking as well as the SDN paradigm's flexibility. The authors haven't defined any behaviors/rules in IoT-SDNPP in prior and have preserved the IoT-based smart city from privacy breaching and loss of data. Finally, they have evaluated the superiority of the proposed model in terms of communication cost.

III. PROPOSED DATA PRIVACY PRESERVATION: ARCHITECTURE AND OBJECTIVE FUNCTION

A. Objective Function

The foremost objective of this research work is to enhance the privacy of the sensitive data in IoT by means of generating an optimal key. The objective model (Obj) of the current research work is expressed mathematically as per Eq. (1).

$$Obj = Min(J) \tag{1}$$

Where J is expressed in Eq. (2), in which the original data R, sanitized data S and the data to be preserved (sensitive data) H are included. The count of data is symbolized as N.

$$J = Min\left(\frac{\sum_{i=1}^{N} S}{\sum_{i=1}^{N} R} - \left[\frac{\sum_{i=1}^{N} R - \sum_{i=1}^{N} H}{\sum_{i=1}^{N} R}\right]\right) \tag{2}$$

B. Adopted Architecture

The step by step procedures for the proposed PPDM model in IoT are as follows:

- Initially the proposed data preservation model includes two processes: (i) Data Hiding and (ii) Data Restoration.
- The data hiding process takes place initially in the sender side and for this sanitization process, a key is required.
- The generated key has to be transformed to its binary value with a length equivalent to the length of data.
- Then, the encrypted sensitive data passes to the receiver side over a defined transmission line.
- The authorized person in the receiver end can get the original data by deploying the inverse key.
- Moreover, the key that used for data sanitization should be optimal, thereby enhances the correlation between the original data and the restored data.

The schematic diagram of the proposed PPDM model in IoT is illustrated in Fig.1.

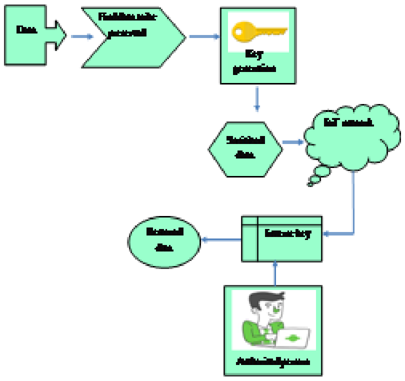


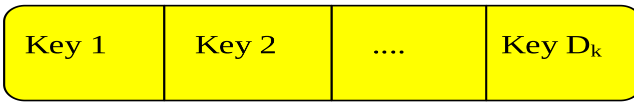
Fig. 1.Architecture of Proposed Privacy Preservation Framework

IV. PROPOSED IMPROVED DRAGONFLY FOR OPTIMAL KEY GENERATION

A. Solution Encoding

The optimal key generation is the major idea behind this work. For the optimal selection, a new IDA is introduced that selects the optimal or best key among the random keys given as the solution (illustrated in Fig 2). More particularly, IDA intakes the count of keys ranging from 1 to D_k. Here, the minimum boundary limit is 1 and the maximum boundary limit is 2^n-1. The length of the solution is expressed mathematically as per Eq. (3).

$$\text{Length of chromosome} = \frac{C_1}{40} \times C_2 \tag{3}$$



Key 1	Key 2	....	Key D_k

Fig. 2.Solution Encoding

B. Improved Dragonfly

Standard DA: The traditional DA is based on the swarming behavior (Static swarm and dynamic swarm) of dragonflies [21]. Here, in the exploration as well as the exploitation phase, a crucial role is played by the randomization process. The major advantage of DA is its capability to neglect out the local optima and get global optimal solution for solving both the constrained or unconstraint optimization problems. The separation (P_i), alignment (A_i), cohesion (G_i) phenomena of DA is mathematically defined in Eq. (4), Eq. (5) and Eq. (6), respectively. Here, the term X denotes the position of the current search agent and X_j reveals the j^{th} position of neighboring search agent. The count of the neighboring individuals is symbolized as N and the velocity of the neighbouring individual in Eq. (5) is represented using the term Q_j.

$$P_i = -\sum_{j=1}^{N} X - X_j \tag{4}$$

$$A_i = \frac{\sum_{j=1}^{N} Q_j}{N} \tag{5}$$

$$G_i = \frac{\sum_{j=1}^{N} X_j}{N} - X \tag{6}$$

The attraction of the search agents towards the food and the distraction of the search agent away from the enemy are expressed as per Eq. (7) and Eq. (8), respectively. Here, the notation *food* and *Enemy* represents the position of the food source and the position of the enemy, respectively.

$$F_i = food - X \tag{7}$$

$$E_i = Enemy + X \tag{8}$$

The position vector (X) and the step vector (ΔX) are taken into consideration to update the position of dragonflies in the exploration phase. Eq. (9) depicts the mathematical formula for the movement of dragonflies. The term P_i, A_i, G_i, F_i and E_i denotes the separation, alignment, cohesion, food source and enemy source of i^{th} individual. In addition, the weight of separation, weight of alignment, weight of cohesion, food factor, enemy factor and weight of i^{th} individual are depicted using the term p, a, g, f, e and w, respectively. The position vector of dragonflies is denoted mathematically as per Eq. (10).

$$\Delta X_{t+1} = \left(pP_i + aA_i + gG_i + fF_i + eE_i\right) + w\Delta X_t \tag{9}$$

$$X_{t+1} = X_t + \Delta X_{t+1} \tag{10}$$

When there is no neighboring solution, the dragonflies make a random walk (Le´vy flight). This random walk is introduced to enhance the randomness, exploration and stochastic behavior. The position update of the dragonflies using a random walk is mathematically shown in Eq. (11).

$$X_{t+1} = X_t + Levy(z) \times X_t \tag{11}$$

The mathematical formula for Levy flight $(Levy)$ is expressed in Eq. (12). Here, r_1 and r_2 are the two arbitrary numbers that reside in the range [0,1]. In addition, β is a constant and δ can be mathematically expressed as per Eq. (13), in which $\Gamma(x) = (x-1)$.

$$Levy(x) = 0.01 \times \frac{r_1 \times \delta}{|r_2|^{\frac{1}{\beta}}} \tag{12}$$

$$\delta = \left(\frac{\Gamma(1+\beta) \times \sin\left(\frac{\pi\beta}{2}\right)}{\Gamma\frac{(1+\beta)}{2} \times \beta \times 2^{\left(\frac{\beta-1}{2}\right)}} \right)^{\frac{1}{\beta}} \tag{13}$$

Improved DA: Besides the advantages of DA**,** the model suffers from the drawback of lower convergence rate. Thus, to override these drawbacks, the improved DA is introduced in this research work.

Assumption: Let the best dragonfly be X_{Best} and the worst dragonfly is denoted as X_{Worst}.

Controversy to traditional*:* In the traditional DA, the value of p, a, g, f, e and w are once updated, the computation of the values of P, A and G takes place using Eq. (4)- Eq. (6), respectively. In the proposed model, in addition to the food position, the fitness position is taken into consideration and it is compared with the threshold fitness (Fit_{th}) as per Eq. (14).

$$Fit_{th} = food\ fitness + (food\ fitness * 0.2) \tag{14}$$

Hence the attraction of X_{Best} towards the food will be minimum and the distraction of X_{Best} from enemy will be maximum. In addition, the updating of the neighboring radius (rad) takes place. In case of the existence of a neighbor, the velocity updating is accomplished using Eq. (6) and Eq. (7), respectively.

The distance from $X_{Best}{}^{th}$ position to food position is depicted using the term Dis_{food} and the Distance from X_{Best} fitness to food fitness is depicted using the term Fit_{food}. Similarly, the Distance from $X_B{}^{th}$ position to enemy position be depicted using the term Dis_{enemy} and Distance from $X_B{}^{th}$ fitness to enemy fitness be symbolized as Fit_{enemy}. The pseudo-code of the proposed IDA approach is depicted in Algorithm 1. The flowchart of the proposed IDA approach is depicted in Fig.3.

Algorithm 1: Proposed Improved DA

```
Initialization: Population of $X_i(i=1,2,...n)$ and step vectors $\Delta X_i(i=1,2,...n)$
Condition 1: in case of end condition being unsatisfied
    Compute: objective value of entire dragonflies
    Update: Source of enemy and food
    Update : the values of $p, a, g, f, e$ and
    Evaluate: $P, A, G$ using Eq. (4-6)
    Condition 2: If $Dis_{food} < rad$ and $Fit_{food} \geq Fit_{th}$
        Evaluate $F$ using Eq. (7)
    Else
        $F$ =zeros ( $x$,1 )
    Condition 3: If $Dis_{enemy} < rad$ and $Fit_{enemy} \geq Fit_{th}$
        Compute: $E$ using Eq. (8)
    Else
        $E$ =zeros ( $x$,1 )
    Update: the radius of the neighbor
    Condition 4: if a dragonfly involves one neighbor dragonfly,
        Update : Velocity of dragonflies are updated using Eq .(9) and position using Eq. (10)
    else
        Update: using Eq. (11) update the position vector
    end if
    Verify and approve the novel positions depending on variable boundaries
end while
```

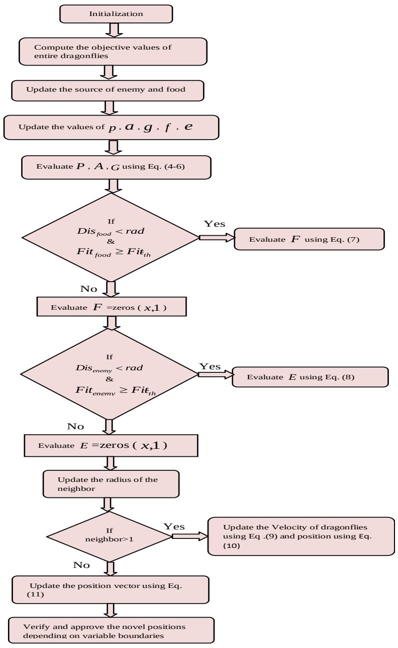

Initialization
Compute the objective values of entire dragonflies
Update the source of enemy and food
Update the values of p, a, g, f, e
Evaluate P, A, G using Eq. (4-6)
If $Dis_{food} < rad$ & $Fit_{food} \geq Fit_{th}$
Yes
Evaluate F using Eq. (7)
No
Evaluate F =zeros (x,1)
If $Dis_{enemy} < rad$ & $Fit_{enemy} \geq Fit_{th}$
Yes
Evaluate E using Eq. (8)
No
Evaluate E =zeros (x,1)
Update the radius of the neighbor
If neighbor>1
Yes
Update the Velocity of dragonflies using Eq .(9) and position using Eq. (10)
No
Update the position vector using Eq. (11)
Verify and approve the novel positions depending on variable boundaries

Fig. 3. Flowchart of the proposed IDA approach

The algorithm steps are described below:

Step 1: Initialize the population of $X_i(i=1,2,...n)$ and step vectors $\Delta X_i(i=1,2,...n)$.

Step 2: Compute the objective values of entire dragonflies

Step 3: Update the source of enemy and food.

Step 4: Update the values of p, a, g, f, e and evaluate P, A, G using Eq. (4-6).

Step 5: If $Dis_{food} < rad$ and $Fit_{food} \geq Fit_{th}$, evaluate F using Eq. (7), else F =zeros (x,1).

Step 6: If $Dis_{enemy} < rad$ and $Fit_{enemy} \geq Fit_{th}$, compute E using Eq. (8), else E =zeros (x,1).

Step 7: Update the radius of the neighbour.

Step 8: If a dragonfly involves one neighbor dragonfly, then update the velocity of dragonflies using Eq. (9) and position using Eq. (10), else update the position vector using Eq. (11).

Step 9: Verify and approve the novel positions depending on variable boundaries.

V. DATA HIDING AND DATA RESTORATION: ARCHITECTURAL DESCRIPTION

A. Data Hiding

With the generated optimal key, the sensitive data that need to be transmitted from the sender over IoT network need to be hidden. Before the hiding of the sensitive data, the chosen optimal key is converted into a binary value.

The specific process that is deployed for the formulation of the binary data is given in the subsequent section:

- The size of data is $C_1 \times C_2$, where the range of data is 200×4. Here, the records be symbolized as C_1 and the fields be denoted as C_2.
- The optimal size of the key is assumed as 20×1, which is multiplied with the original data to generate the hidden or sanitized data.
- Then, the key that is subjected to further processing is converted into its corresponding binary form. For accomplishing the equivalent binary form, the optimal key of size 20×1 is converted into five subsets with 4 elements in each. Each of the elements in the 5 subsets is is transformed into 40 binary bits. Therefore, each subset achieves (40×4) data and as a whole, there is five (40×4) data. These five (40×4) data is said to be the generated binary data.
- Further, to acquire the cumulative binary data of size (200×4), the concatenation of five (40×4) data takes place.
- Finally, the sensitive data is generated by means of multiplying the original sensitive data with the product of the binary data.

B. Data Restoration

The two major components of the generated optimal key are index and sensitive data. A vector corresponding to the sanitized data having the length alike the length of the sanitized data is generated in the data restoration process and it is then multiplied with the optimal key index. Further, the restored data or the original data is acquired by means of summing the sanitized data with the multiplied data.

Moreover, in the case of the generated optimal key being more accurate, the recovering of the original data takes place more efficiently.

Apart from this, in case of the key produced being inaccurate, then there is no chance for the accurate restoration of the original data. Moreover, to reveal the significance of the projected IDA in optimal key generation, the correlation coefficient is computed for both the recovered and original data.

VI. RESULTS AND DISCUSSION

A. Simulation procedure

The proposed data privacy model in IoT was implemented in MATLAB and the results acquired are observed algorithmically. The proposed model was evaluated using the physical activity data monitoring and here the size of each data is [600 ×4], i.e. 600 records and 4 fields. From the original data, the synthetic data is formulated and it is varied along 10%, 20%, and 30% respectively. Subsequently, from this variation, three test cases, viz. Test case1, Test case 2 and Test case 3 are generated. The arbitrary data are generated for each of the variations. That is, in the case of 10% variation, the random data is generated within the range (-10 to +10) by means of either adding or subtracting the values. Similar to this for 20% and 30% variation, the random data is generated within the range of (-20 to +20) and (-30 to +30), respectively.

B. Convergence analysis in terms of Enemy Distraction Weight (e) and Food Attraction Weight (f)

Enemy Distraction Weight: The convergence analysis of the proposed model under varied enemy distraction weight (e) is shown in Table I by varying the count of iterations from 0 to 100. Here, in case of Test Case 1 in Table I, at 100th iteration, the highest cost function is achieved when $e=0.098$ and it is 50%, 5%, 12.5%, and 37.5% better than the convergence obtained in proposed model when $e=0.0$, $e=0.0245$, $e=0.049$ and $e=0.0735$, respectively. Similar to this in Fig. 4(b), for Test case 2, the highest cost function is achieved when $e=0.049$ and it is 80%, 8%, 10% and 40% superior to the performance when $e=0.0245$, $e=0.0735$, $e=0.098$ and $e=0.0$, respectively at 100th iteration.

Table. I. Convergence analysis of Proposed work for different enemy distraction weight (e) on (a) Testcase I (b) Testcase II (c) Testcase III

Test case 1						
weights	0%	20%	40%	60%	80%	100%
$e=0.0$	1.4825	0.2775	0.3547	0.2263	0.2155	0.2453
$e=0.0245$	1.4646	0.4359	0.4246	0.3451	0.3822	0.3891
$e=0.049$	1.4513	0.3998	0.4125	0.3725	0.3598	0.3255
$e=0.0735$	1.4278	0.3596	0.2454	0.2358	0.3854	0.2369
$e=0.098$	1.4043	0.3973	0.3922	0.3972	0.3712	0.4215
Test case 2						
weights	0%	20%	40%	60%	80%	100%
$e=0.0$	1.4878	0.4235	0.4125	0.3841	0.3732	0.3751
$e=0.0245$	1.4791	0.4836	0.4769	0.3456	0.3145	0.3124
$e=0.049$	1.4887	0.5867	0.4691	0.4256	0.4264	0.42258
$e=0.0735$	1.4799	0.3764	0.4854	0.4325	0.4351	0.4458
$e=0.098$	1.4981	0.4694	0.4596	0.4478	0.4654	0.4521
Test case 3						
weights	0%	20%	40%	60%	80%	100%
$e=0.0$	1.4581	0.3541	0.4325	0.3981	0.3732	0.3754
$e=0.0245$	1.42345	0.4123	0.4695	0.3254	0.3846	0.3751
$e=0.049$	1.4852	0.4846	0.5129	0.3169	0.3654	0.3694
$e=0.0735$	1.4692	0.4676	0.3847	0.3875	0.4213	0.4216
$e=0.098$	1.43494	0.3659	0.4521	0.4426	0.3954	0.3951

Food Attraction Weight: The convergence analysis of the proposed model under varied food attraction weight (f) is computed by varying the count of iterations from 0 to 100 as per Table II. In order to achieve the objective of privacy preservation, the attraction towards the food source needs to be lower. Here, for Test case 1 in Table II, the lowest cost function is achieved when $f=0.024$ at 100th iteration and it is 33.3%, 25%, 14.2%, and 10.8% better than the performance of the proposed IDA, when $f=0.049$, $f=0.0$, $f=0.0735$ and $f=0.098$, respectively. This section clearly exhibited the cost function evaluation of enemy distraction weight (e) and food attraction weight (f).

Table. II. Convergence analysis for IDA in terms of food attraction weight (f) on (a) Testcase I (b) Testcase 2 (c) Testcase 3

Test case 1						
weights	0%	20%	40%	60%	80%	100%
$e=0.0$	1.4988	0.4153	0.4153	0.4153	0.4153	0.4153
$e=0.0245$	1.4875	0.4352	0.4231	0.2981	0.2981	0.2981
$e=0.049$	1.4836	0.4251	0.4253	0.4253	0.4253	0.4253
$e=0.0735$	1.4945	0.4469	0.4469	0.4321	0.4295	0.4168
$e=0.098$	1.4658	0.4256	0.4256	0.4256	0.4256	0.4256
Test case 2						
weights	0%	20%	40%	60%	80%	100%
$e=0.0$	1.4845	0.6546	0.6546	0.6546	0.6546	0.6546
$e=0.0245$	1.4866	0.4023	0.4023	0.3589	0.3589	0.3589
$e=0.049$	1.4924	0.4251	0.4251	0.3654	0.3654	0.3654
$e=0.0735$	1.4963	0.4523	0.4523	0.3654	0.3654	0.3654
$e=0.098$	1.4997	0.4564	0.4564	0.312	0.298	0.3254
Test case 3						
weights	0%	20%	40%	60%	80%	100%
$e=0.0$	1.4899	0.2863	0.2863	0.2863	0.2863	0.2863
$e=0.0245$	1.4887	0.3125	0.3125	0.3125	0.3125	0.3125
$e=0.049$	1.4955	0.4035	0.4126	0.3742	0.3638	0.3672
$e=0.0735$	1.4952	0.3696	0.4245	0.4321	0.3742	0.2892
$e=0.098$	1.4966	0.4426	0.4426	0.3786	0.3786	0.3786

C. Key sensitivity Analysis

Table III exhibits the key sensitivity analysis of the enemy distraction weight (e) for the proposed IDA model for 10%, 30%, 40% and 70% of variation. This evaluation is conducted for 3 Test cases, viz. Test case1, Test case2 and Test case 3, respectively. In the case of Test case 1 at 40% of variation, the proposed IDA achieves the maximum value at $e=0.0$ and the corresponding value is 0.77424 and it is 1.87%, 0.04%, 1.82% and 2.6% better than $e=0.098$, $e=0.0735$, $e=0.049$ and $e=0.0245$, respectively.

The key sensitivity evaluation of the proposed IDA approach for food attraction weight (f) in terms of 10%, 30%, 40% and 70% of variation corresponding to 3 Test cases is exhibited in Table IV. Here, the lowest value of f in IDA is observed under Test case 3 at 70% as 0.75186 in $f=0.098$, which is 6.19%, 5.13%, 6.83% and 4.75% better than the performance of the proposed IDA, when $f=0.0$, $f=0.024$, $f=0.049$ and $f=0.0735$, respectively.

TABLE III KEY SENSITIVITY ANALYSIS OF THE PROPOSED IDA IN TERMS OF ENEMY DISTRACTION WEIGHT (e) FOR TEST CASE 1, TEST CASE 2 AND TEST CASE 3

Test case 1				
	10%	30%	40%	70%
$e=0.0$	0.89889	0.72017	0.77424	0.71794
$e=0.0245$	0.9024	0.72568	0.75388	0.71656
$e=0.049$	0.90494	0.73614	0.76013	0.7235
$e=0.0735$	0.9012	0.73245	0.77037	0.73261
$e=0.098$	0.90098	0.72267	0.75969	0.72042
Test case 2				
	10%	30%	40%	70%
$e=0.0$	0.93503	0.73112	0.79127	0.78317
$e=0.0245$	0.93881	0.74285	0.79236	0.76149
$e=0.049$	0.93768	0.72822	0.80305	0.79033
$e=0.0735$	0.93645	0.73009	0.78695	0.78227
$e=0.098$	0.93357	0.71157	0.7872	0.78534
Test case 2				
	10%	30%	40%	70%
$e=0.0$	0.97794	0.85077	0.69692	0.79782
$e=0.0245$	0.97477	0.85331	0.68916	0.78422
$e=0.049$	0.97524	0.85807	0.69829	0.77589
$e=0.0735$	0.97523	0.84446	0.68372	0.73866

$e = 0.098$	0.97417	0.8541	0.68946	0.77429

TABLE IV KEY SENSITIVITY ANALYSIS OF THE PROPOSED IDA IN TERMS OF FOOD ATTRACTION WEIGHT (f) FOR TEST CASE 1, TEST CASE 2 AND TEST CASE 3

Test case 1				
	10%	30%	40%	70%
$f = 0.0$	0.9802	0.88654	0.74263	0.73056
$f = 0.0245$	0.98245	0.8869	0.75507	0.68995
$f = 0.049$	0.98366	0.89449	0.76325	0.73405
$f = 0.0735$	0.98197	0.88638	0.75201	0.72519
$f = 0.098$	0.98194	0.88426	0.74307	0.70121
Test case 2				
	10%	30%	40%	70%
$f = 0.0$	0.94223	0.77581	0.77716	0.71182
$f = 0.0245$	0.94851	0.78113	0.78012	0.72826
$f = 0.049$	0.94017	0.76777	0.75042	0.71092
$f = 0.0735$	0.94293	0.78369	0.76718	0.73442
$f = 0.098$	0.94636	0.78731	0.76597	0.72226
Test case 3				
	10%	30%	40%	70%
$f = 0.0$	0.94038	0.86051	0.74272	0.8015
$f = 0.0245$	0.94162	0.83764	0.73636	0.79258
$f = 0.049$	0.94561	0.84672	0.73231	0.80699
$f = 0.0735$	0.94361	0.85295	0.71204	0.78941
$f = 0.098$	0.93899	0.83908	0.69167	0.75186

D. Attack Analysis: KPA and CPA

This section portrays about the attacks like KPA and CPA. The analysis on KPA is accomplished by correlating original data with all original data and sanitized data with all sanitized data. In addition, the CPA analysis is undergone by correlating each sanitized data with its corresponding restored data. The attack analysis (both KPA and CPA) of the proposed IDA model is evaluated algorithmically for 3 Test cases and is tabulated. Table V exhibits the KPA analysis for Test case 1, test case 2 and Test case 3, respectively in terms of varying enemy distraction weight (e) form $e = 0.098$, $e = 0.0$, $e = 0.049$, $e = 0.0735$ and $e = 0.0245$, respectively and food attraction weight (f) from $f = 0.049$, $f = 0.0$, $f = 0.0735$ and $f = 0.098$ and $f = 0.024$, respectively. For a typical privacy model, the KPA and CPA need to be lower.

TABLE V KPA AND CPA ANALYSIS OF PROPOSED IDA FOR ENEMY DISTRACTION WEIGHT (e) AND ENEMY DISTRACTION WEIGHT (e)

KPA Attack				CPA Attack			
Enemy				Enemy			
Enemy Distraction Weight	Test Case 1	Test Case 2	Test Case 3	Enemy Distraction Weight	Test Case 1	Test Case 2	Test Case 3
$e = 0.0$	0.98647	0.84825	0.98847	$e = 0.0$	0.98796	0.77233	0.94653
$e = 0.0245$	0.9918	0.9904	0.99657	$e = 0.0245$	0.79438	0.95093	0.92618
$e = 0.049$	0.99876	0.96598	0.94895	$e = 0.049$	0.959	0.92474	0.86545
$e = 0.0735$	0.97733	0.96522	0.95651	$e = 0.0735$	0.93012	0.92619	0.97484
$e = 0.098$	0.99555	0.98243	0.87654	$e = 0.098$	0.9869	0.96243	0.99346
Food				Food			
Food Attraction Weight	Test Case 1	Test Case 2	Test Case 3	Food Attraction Weight	Test Case 1	Test Case 2	Test Case 3
$f = 0.0$	0.99596	0.98217	0.99344	$f = 0.0$	0.95711	0.98685	0.9611
$f = 0.0245$	0.96681	0.98288	0.99589	$f = 0.0245$	0.93709	0.99436	0.90861
$f = 0.049$	0.99604	0.97692	0.97071	$f = 0.049$	0.96738	0.90849	0.89809
$f = 0.0735$	0.99178	0.98344	0.99734	$f = 0.0735$	0.96833	0.86442	0.97115
$f = 0.098$	0.96916	0.99268	0.99206	$f = 0.098$	0.79337	0.97297	0.96983

VII. CONCLUSION

The current research work on IoT privacy preservation has an improved data sanitization and restoration framework with the intention of achieving higher-order privacy preservation. The data preservation process was using the optimally selected key. As a novelty, the key was optimally selected by introducing IDA, which was the extended version of DA.

Finally, the algorithmic analysis was carried out by varying parameters like enemy distraction weight (e) and food attraction weight (f) of proposed algorithm. In case of Test Case 1 at 100th iteration, the highest cost function is achieved when $e = 0.098$ and it is 50%, 5%, 12.5% and 37.5% better than the convergence obtained when $e = 0.0$, $e = 0.0245$, $e = 0.049$ and $e = 0.0735$, respectively. For Test case 2, the highest cost function is achieved when $e = 0.049$ and it is 80%, 8%, 10% and 40% superior to the performance

when $e = 0.0245$, $e = 0.0735$, $e = 0.098$ and $e = 0.0$,respectively at 100th iteration. Thus the enhancement of the proposed algorithm was confirmed by various research analyses in preserving data in IoT.

REFERENCES

1. Zhitao Guan, Yue Zhang, Longfei Wu, Jun Wu, Jingjing Hu,"APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT",Journal of Network and Computer Applications, vol.125,pp.82-92,January 2019.
2. Vishal Sharma, Ilsun You, Dushantha Nalin K. Jayakody, Mohammed Atiquzzaman,"Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of Things",Future Generation Computer Systems, vol.92,pp.758-776,March 2019.
3. Konev Anatoly, Khaydarova Rezeda, Lapaev Maxim, Luanye Feng, Bondarenko Igor,"CHPC: A complex semantic-based secured approach to heritage preservation and secure IoT-based museum processes",Computer Communications, vol.148,pp240-249,December 2019.
4. Yuhang Wang,Hongli Zhang,Shen Su,"VAT: A Velocity-Aware Trajectory Privacy Preservation Scheme for IoT Searchin", Cloud Computing and Security,pp.357-365, September 2018
5. Mehdi Gheisari,Guojun Wang,Shuhong Chen,Hamidreza Ghorbani,"IoT-SDNPP: A Method for Privacy-Preserving in Smart City with Software Defined Networking",Algorithms and Architectures for Parallel Processing, pp 303-312,December 2018.
6. X. Zhang, C. Liu, S. Poslad and K. K. Chai, "A Provable Semi-Outsourcing Privacy Preserving Scheme for Data Transmission From IoT Devices," IEEE Access, vol. 7, pp. 87169-87177, 2019.
7. M. Yang, T. Zhu, Y. Xiang and W. Zhou, "Density-Based Location Preservation for Mobile Crowdsensing With Differential Privacy," IEEE Access, vol. 6, pp. 14779-14789, 2018.
8. A. Soltani Panah, A. Yavari, R. van Schyndel, D. Georgakopoulos and X. Yi, "Context-Driven Granular Disclosure Control for Internet of Things Applications," IEEE Transactions on Big Data, vol. 5, no. 3, pp. 408-422, 1 Sept. 2019.
9. Muneeb Ul Hassan, Mubashir Husain Rehmani, Jinjun Chen,"Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions",Future Generation Computer Systems,vol.97,pp.512-529,August 2019
10. Xiaolong Xu, Shucun Fu, Lianyong Qi, Xuyun Zhang, Shancang Li,"An IoT-Oriented data placement method with privacy preservation in cloud environment",Journal of Network and Computer Applications, vol.124,pp.148-157,December 2018
11. Yi-Ning Liu, Yan-Ping Wang, Xiao-Fen Wang, Zhe Xia, Jing-Fang Xu ,"Privacy-preserving raw data collection without a trusted authority for IoT",Computer Networks, Vol.148,pp340-348, January 2019.
12. Gang Sun, Victor Chang, Muthu Ramachandran, Zhili Sun, Dan Liao ,"Efficient location privacy algorithm for Internet of Things (IoT) services and applications",Journal of Network and Computer Applications,vol.89,pp.3-13,July 2017.
13. Zhiwei Wang,"A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity",Future Generation Computer Systems, Vol.82,pp342-348,May 2018.
14. Rafik Hamza, Zheng Yan, Khan Muhammad, Paolo Bellavista, Faiza Titouna,"A privacy-preserving cryptosystem for IoT E-healthcare",Information Sciences, in comm unication, 2019.
15. Fei Zhu, Wei Wu, Yuexin Zhang, Xiaofeng Chen,"Privacy-preserving authentication for general directed graphs in industrial IoT",Information Sciences, Vol.502,pp218-228,October 2019
16. Karam Bou Chaaya, Mahmoud Barhamgi, Richard Chbeir, Philippe Arnould, Djamal Benslimane,"Context-aware System for Dynamic Privacy Risk Inference: Application to smart IoT environments",Future Generation Computer Systems, vol.101,pp.1096-1111,December 2019
17. Sana Moin, Ahmad Karim, Zanab Safdar, Kalsoom Safdar, Muhammad Imran ,"Securing IoTs in distributed blockchain: Analysis, requirements and open issues",Future Generation Computer Systems, Vol.100,pp. 325-343,November 2019
18. Valentin Tudor, Vincenzo Gulisano, Magnus Almgren, Marina Papatriantafilou,"BES: Differentially private event aggregation for large-scale IoT-based systems",Future Generation Computer Systems, in communication, 2019.
19. Ming Tao, Jinglong Zuo, Zhusong Liu, Aniello Castiglione, Francesco Palmieri,"Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes",Future Generation Computer Systems,vol.78,part 3, pp. 1040-1051,January 2018.
20. Marcus Walshe, Gregory Epiphaniou, Haider Al-Khateeb, Mohammad Hammoudeh, Ali Dehghantanha,"Non-interactive zero knowledge proofs for the authentication of IoT devices in reduced connectivity environments",Ad Hoc Networks,vol.95,December 2019.
21. Mohammad Jafari, Mohammad Hossein and Bayati ChaleshtariM.Sc, "Using dragonfly algorithm for optimization of orthotropic infinite plates with a quasi-triangular cut-out", European Journal of Mechanics - A/Solids, vol.66, pp.1-14, 2017, November–December 2017.

AUTHOR PROFILE

Ravindra S. Apare is a Research Scholar at Department of Computer Science and Engineering at Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India. His interests are in Internet of Things, Information Cyber Security, Human Computer Interaction and Image Processing. He has received M.E. in Computer Science & Engineering from Department of Computer Science and Engineering, Mahatma Gandhi Mission`s College of Engineering, Swami Ramanand Tirth Marathwada University, Nanded and M.B.A. in Human Resource Management from Indira Gandhi National Open University, Delhi. B.E. in Computer Science & Engineering from Marathwada Institute of Technolgy College of Engineering, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad.

Guide
Dr. Satish N. Gujar is a Research Guide at Department of Computer Science and Engineering, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India. His interests are in Database, Big Data, Internet of Things, Information Cyber Security, Computer Graphics and Image Processing. He has received Ph.D. in Computer Science & Engineering from Department of Computer Science and Engineering, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India. , M.E. in Computer Science and Engineering from Professor Ram Meghe Institute of Technology and Research, Badnera, Amravati. And B.E. in Computer Science & Engineering from Babasaheb Naik College of Engineering, Pusad, Dt. Yavatmal.