SECURITY AND PRIVACY AWARE PROGRAMMING MODEL FOR IOT APPLICATIONS IN CLOUD ENVIRONMENT

Subba Reddy Borra[1], Smitha Khond [1] and D .Srivalli [2]

[1]Department of Computer Science and Engineering, Malla Reddy Engineering College for Women (Autonomous), Hyderabad, Telangana, India.
[2]Department of Information Technology, Malla Reddy Engineering College for Women (Autonomous), Hyderabad, Telangana, India

ABSTRACT

The introduction of Internet of Things (IoT) applications into daily life has raised serious privacy concerns among consumers, network service providers, device manufacturers, and other parties involved. This paper gives a high-level overview of the three phases of data collecting, transmission, and storage in IoT systems as well as current privacy-preserving technologies. The following elements were investigated during these three phases:(1) Physical and data connection layer security mechanisms(2) Network remedies(3) Techniques for distributing and storing data. Real-world systems frequently have multiple phases and incorporate a variety of methods to guarantee privacy. Therefore, for IoT research, design, development, and operation, having a thorough understanding of all phases and their technologies can be beneficial. In this Study introduced two independent methodologies namely generic differential privacy (GenDP) and Cluster-Based Differential privacy (Cluster-based DP) algorithms for handling metadata as intents and intent scope to maintain privacy and security of IoT data in cloud environments. With its help, we can virtual and connect enormous numbers of devices, get a clearer understanding of the IoT architecture, and store data eternally. However, due of the dynamic nature of the environment, the diversity of devices, the ad hoc requirements of multiple stakeholders, and hardware or network failures, it is a very challenging task to create security-, privacy-, safety-, and quality-aware Internet of Things apps. It is becoming more and more important to improve data privacy and security through appropriate data acquisition. The proposed approach resulted in reduced loss performance as compared to Support Vector Machine (SVM) , Random Forest (RF) .

KEYWORDS

Cloud Computing, IoT Applications, Security, Privecy, IoT Systems, Generic Diffential Privecy(GenDP), Cluster Based Diffential Privacy(Cluster-based).

1. INTRODUCTION

The two types of privacy are physical privacy and informational privacy. Data security, which prevents unauthorised access to data while it is being stored and transmitted across a network, and information privacy, which deals with the security of personal data, are two concepts that are related to one another. Data security and privacy are related because data may include personal information about an individual. Privacy also depends on the social context of the data. These privacy concerns have grown as a result of the Internet of Things. Personal information leaks can happen directly or indirectly. The direct disclosure of personal information, such as sensitive data, location, and identity, can lead to privacy threats in terms of tracking, localising, and personalising. A variety of data mining techniques for indirect data violations use content

analysis. Bad behaviour on the part of IoT system owners (or service owners) can lead to significant direct and indirect privacy leaks.

This essay discusses the conundrum of application placement and user assignment. We also include a range of security and privacy constraints, such as I location constraints at the module, user, and co-location levels, (ii) co-location constraints, and (iii) k-anonymity constraints, in addition to capacity and latency constraints. We formalise the problem and develop a mixed integer programming solution that is quadratically constrained. We illustrate the applicability of the suggested strategy using an IoT system in the smart home sector. Controlled experiments on problem cases of increasing size show that the algorithm is capable of solving even large issue instances in a fair amount of time[2].

Any banking institution's effectiveness is assessed based on its ability to manage money effectively over the long term and to produce returns via the efficient use of available resources. Additionally, for the purposes of the economy and their customers, banks must have a sufficient amount of liquid assets. Additionally, bank transfers need to be protected in order to avoid negative loan impairment. Therefore, it must be impossible for bank strategies to balance the risks associated with commercial activity. [3] The findings of this study, which used a multi-criteria approach to decision-making, took the fundamental components of financial performance evaluation to understand the managerial banks' capacity, and it was discovered that efficient banks reduce risks, boost profits, and maintain consistency in their operations. However, the dynamic, varied, dispersed, and resource-constrained nature of the edge computing paradigm also brings with it some problems, such as more significant privacy leakages and performance restrictions. How to ensure that the resource requirements of the application are met while enhancing user privacy security to the greatest extent presents a challenge for the job assignment of IoT applications. To address this issue, we propose an IoT job assignment strategy at the network edge. The author here first models the resource and privacy requirements for IoT applications before evaluating the resource satisfaction and privacy compatibility between edge devices and workloads. Second, we analyse the topic of privacy-aware IoT task assignment on edge devices (PITAE) and present two solutions utilising the greedy search approach and the Kuhn-Munkres (KM) algorithm. [4] Even novice programmers may now easily create cloud-connected Internet of Things (IoT) systems thanks to specialised cloud platforms that integrate the necessary components of an IoT system. In this environment, a growing number of Internet of Things (IoT) technologies are being developed and deployed over open networks, frequently with insufficient security. A quick user study revealed that inexperienced IoT programmers in particular commonly overlook security problems. In order to address this risk, the study looks at the security features provided by two major cloud-IoT platforms (Amazon Web Services and Microsoft Azure). It then focuses on the configurations, tools, and processes designed to produce more secure deployments. [5]We discovered that these platforms could effectively address numerous security vulnerabilities identified in the study, if the appropriate characteristics were identified and used. The paper concludes by offering a set of suggestions to help novice IoT developers avoid the most common and ongoing security difficulties in their work and make better use of the built-in security features of cloud-IoT platforms. a generalisation based on probability theory to handle the dimensionality issue with high-dimensional data[5]. By dividing the noisy cell data with Laplace noise, the DPCube approach, which uses the KD-tree partitioning algorithm for multi-dimensionality health data, produced a differentially personalised cell histogram. However, due to the large domain values and attributes in multi-dimensional data, multi-dimensional partitioning causes an increase in estimation errors[6]. We discovered that these platforms might effectively address many of the security vulnerabilities identified in the study if the correct features were discovered and used. A list of recommendations is the study's last contribution. From bottom to top, IoT architecture typically consists of three levels: perception, network, and application. These layers provide data sensing, data communication,

and data processing for various IoT devices and applications. The network layer connects devices to the network in order to analyse and transmit sensor data. It offers customers services catered to particular applications [7]. The device's sensors detect and gather information, including physical parameters, gathered from the environment. specifically observations of common datasets in the topic of privacy budget burnout. However, compressed sensing, where sparse tree reconstruction is undesirable and privacy protection flaws exist, was where their solution fell short[8]. These performed admirably with multi-dimensional data but struggled with large amounts of data. For the introduction of an effective differential private privacy method for publishing high-dimensional data, these methods place a large informational burden. Because of things like device failure, network problems, and implausible sensor data, applications for the Internet of Things (IoT) are vulnerable to extreme environments. We examine how component and connector (C&C) architectures with built-in encapsulation might be used to develop and deploy dependable IoT applications. Current C&C languages for building IoT applications mostly focus on outlining architectures and delivering parts to IoT devices. Additionally, similar approaches usually confine the models to a particular platform and contaminate them with low-level implementation details, making them more challenging to understand[9]. The error-handling strategies improved the dependability of C&C-based IoT systems without adding time-consuming error-handling code that makes the models difficult to understand, especially for non-experts. However, there are various security and privacy problems when sharing personally identifiable health information (PHI) to others. This is especially true when using next-generation healthcare platforms, such as mobile healthcare social networks (MHSNs). The authors recommended [10] scalable and fine-grained data access control to ensure that patients have full control over their PHI. PHI sharing typically gives information about owners or recipients. Attribute-based encryption is the foundation of the proposed paradigm. The suggested approach takes use of attributes with a name and a value, and it effectively uses a Bloom filter to look at the attributes prior to decryption. Therefore, the suggested strategy maintains the policy and data privacy. The suggested solution outsources attribute-based encryption & decryption to the cloud while restricting the cloud from reading content and access restrictions since it considers that the complexity of access regulations increases the computational cost and energy & resource limits in smart phones. The experimental results show that the performance analysis and security of the suggested approach hold the fine-grained access policies for PHI sharing. Even though the proposed EPPS might offer fine-grained access control, cloud-based hidden access controls ought to be straightforward to implement on mobile devices with constrained resources[11]. Numerous Internet of Things (IoT) platforms have been created in accordance with diverse design concepts, computing paradigms, technologies, and objectives in an effort to streamline and speed up the development of the IoT ecosystem. This article will explore the key IoT platform examples that make up the varied IoT platform landscape and compare them using the IoT-A reference architecture. Regardless of their low-level specifications, heterogeneous IoT platforms (both current and future) can be analysed in this way by concentrating only on the core architectural features and functionalities that permit communication among stakeholders, software, data flow, and hardware within the IoT ecosystem. The algorithms developed to protect the differential privacy of IoTmeta data in a cloud context are divided into interactive and non-interactive techniques in the existing literature. The data miner can dump aggregate requests using a safe, private approach using the interactive technique, and the server will send answers as needed. The majority of the currently used techniques employ an interactive framework for varying privacy and security. In a non-interactive manner, the server first makes the metadata anonymous before making it available to users. Using cluster analysis and the similarity of the attribute behaviours, we use a non-interactive approach of differential privacy in this manuscript and publish the contingency tables or marginals of the metadata. However, this approach works well for high-dimensional metadata with a broad domain[12]. In order to offer a different level of privacy protection The use of diverse health data is suggested with a non-interactive manner. The primary objective of data release or publication is to safeguard the privacy of the crucial component, and

it is crucial that the efficacy of the published data is also protected. To successfully personalise for safeguarding information in data mining applications, a cluster-based privacy-preserving technique for metadata is presented.

1. It is clear from the literature that there is no differential privacy technique that allows simultaneous access to IoT meta-data or relational data. As a result, the suggested differential privacy data algorithm uses generalised techniques to maintain the information in cluster analysis. Deterministic strategies clearly failed to provide -differential privacy since they relied on the distributed data. However, ambiguous processes are also added when publishing differential privacy data.

2. The suggested cluster-based solution accommodates various attribute types and does not call for pre-discretized for numerical attributes. The suggested method establishes the centroids based on the similarity of the attributes in order to provide accurate classification while maintaining -differential privacy. Although the efficacy of the data produced by the various personal differential privacy algorithms has been overlooked, the literature characterises the -differential privacy as a robust privacy protection. The findings of our experiments show that our cluster-based approach to classifier creation offers superior security compared to customised interactive algorithms.

Differential privacy refers to a privacy paradigm that reduces the possibility of individual data being identified and maximises privacy (DP). Using the DP principle, the amount of information that can be disclosed about a person's data that is stored in a database to a third party or enemy can be limited. Epsilon () and delta (), which indicate the level of privacy caused to be by a randomised privacy-preserving algorithm (M) over a particular database, are the traditional symbols for these constraints in DP (D).

Definition 1. (Differential privacy)

A randomized function RF with a well-defined probability density PD satisfies $\epsilon - \text{Differential privacy}$ if, for any two neighboring datasets $DS1$ and $DS2$ that differ by only one record and for any $RE \in range(MR)$

$$PD\ (RF\ (DS1) = RE) \leq e^{\epsilon} * PD\ (RF\ (DS2) = RE)$$

Generally, Laplace mechanism is used to achieve the Differential privacy (DP). To generate Laplace distribution parameters are selected based on global sensitivity and privacy budget.

Definition 2. (Global sensitivity)

Let the database is mapped to a fixed-size vector of real numb using a functionfn. The global sensitivity of fn for all neighboring databases $DS1$ and $DS2$ is computed as

$$\Delta\ (fn) = max_{DS1,DS2} \| fn(DS1) - fn(DS2) \|$$

where$||.||$ denotes the L1 norm.

Noise should be added to response a range query with$\epsilon - DP$. Because one record will contaminate the estimation of the appropriate response by just one, the global sensitivity Δf in our scheme should be 1. Let $Lap(\lambda)$ indicate the Laplace probability distribution with a mean of

zero and scale λ, where $\lambda = \Delta f/\epsilon$.We can add noise sampled from $Lap(\lambda)$ to an original response re to achieve $\epsilon - DP$.

Definition 3. (Laplace mechanism) Let rq be an response to a range query, and let η be a random variable such that $\eta \sim Lap(\delta f/\epsilon)$. The Laplace mechanism is defined as follows:

$$\overline{\mathrm{r\,q}} = \mathrm{r\,q} + \eta.$$

Sequential composition and parallel composition are the two main properties of Differential privacy.

The hypothesis confirms that adding up the precise quantity of noise to statistical queries, one can achieve positive results at the same time provided a quantifiable conception of privacy. According to the definition, it doesn't conform to the rules of syntax from the data rather it is formed by comparing results of a query on any database with or without any one individual: a query Q (a randomized function) is ε-differentially private if the difference in probability of any query outcome on a data-set only varies by a factor of e ε (approximately 1 + ε for small ε) whenever an individual is added or removed. A variety of query mechanisms are developed in literature which provides Differential privacy for quantifiable collection of statistical problems. A little state-of-art has focused private mechanisms on composition principles to design the system. These principles build more complex differentially private building blocks in principled way, so that the resulting programs are guaranteed to be differentially private by construction The initial point for the current state-of –art is PINQ.

2. METHODOLOGY

In this section we introduced two independent methodologies or algorithms for Differential privacy namely generic differential privacy (GenDP) and Cluster-Based Differential privacy (Cluster-basedDP) algorithms. The GenDP provides generalized privacy protection algorithm for homogeneous and heterogeneous meta-data from the IoT applications in Cloud environment. The GenDP algorithm consider intent scope from single intent as homogeneous data and global intent scope is classified asheterogeneous data from diversified sources and this is portioned using portioned algorithm before defining the classifiers for validating the accuracy. The cluster-based DP groups the data into clusters based on the similarity of the behavior or attribute values, later it defines the classifiers for validating the personal or differential privacy.

2.1. Generic Differential Privacy

A variety of partition-based models [13][14]are proposed in the recent literature to prevent the privacy and security of the IoT applications from local and global intent scopes with insecure intents and this provides insufficient protection, because these are vulnerable to several insecure intents. In this paper, a differential privacy (DP) model is proposed which guarantees privacy and protects IoT application data from all intents. This differential privacy (DP) model does not depend on the opponent's background knowledge. The probability of any output (published data) is from identically distributed data from diversified environments and which promises all these outputs are insensitive to any single transaction of intent. This states that the privacy of intent scope is not under risk, because diversified disclosed data set is included. The GEnDp and Portioning algorithms are given in Algorithm1 and Algorithm2.

Algorithm 1: DiffGen

Input: Meta-data set from IoT applicationsDS, privacy budget ε, and number of specializations s

Output: Generalized intent set $\widehat{DS}$

1. Initially, the highest value is assigned to every value of DS
2. The highest value is initially assigned to Ct_i
3. For specification of predictors, Set privacy budget as $\acute{\varepsilon} \leftarrow \frac{\acute{\varepsilon}}{2(|AT_n^{pr}| + 2s)}$
4. Specify the split value for each$va_n \in \cup Ct_i$with probability $\alpha \exp\left(\frac{\acute{\varepsilon}}{2\Delta u} u(DS, va_n)\right)$;
5. Calculate the score for each candidate$\forall\ va \in \cup Ct_i$
6. for $i = 1$ to s do
7. Select $va \in \cup\ Ct_i$ with probability $\alpha \exp\left(\frac{\acute{\varepsilon}}{2\Delta u} u(DS, va)\right)$;
8. Specialize va on DS and update $\cup Ct_i$;
9. for each new$va_n \in \cup Ct_i$, Determine the split value with probability $\alpha \exp\left(\frac{\acute{\varepsilon}}{2\Delta u} u(DS, va_n)\right)$;
10. Update score for$va \in \cup\ Ct_i$;
11. end for
12. each group with count $\left(co + lap\left(\frac{2}{\varepsilon}\right)\right)$ is returned, where $Lap(\cdot)$denotes the probability density function of Laplaciandistribution.

Algorithm 1 Differential-private partition Algorithm

Input:DB_{t_i},TH_D,TH_R,TH_L,$q.\epsilon_i$

Output: intents subsetBU;

1. Initialization: Set $sz = 0; i = 1; j = 1; BU = \phi$;
2. $\widehat{TH_D} = TH_D + ZN, \widehat{TH_R} = TH_R + \overline{ZN}, \lhd\ ZN, \overline{ZN} \sim Lap\ ((q.\epsilon_i))$
3. $bu_j \rightarrow\ db_i; Min = Max = Current =\ db_i; sz++; i++;$
4. while$i \leq length(DB)$do
5. if$Current \neq Null$ and $|Current -\ db_i| > \widehat{TH_R}$then
6. if $bu_{j-1}.length > 1$then
7. ⊳Last bucket is not a single bin bucket
8. $last = BU.pop(); bu_j = lasy.pop();$
9. $BU \leftarrow last; BU \leftarrow bu_j;\ j++;\ bu_j \leftarrow db_i;\ BU \leftarrow bu_j;$
10. $j++; Current = x; i++; sz = 0;$
11. else ⊳Last bucket is a single bin bucket
12. $bu_j \leftarrow x; BU \leftarrow bu_j;$
13. $j++; Current = x; i++; sz = 0;$
14. elseif
15. else if $sz == 1$ then
16. $BU \leftarrow bu_j;\ j++;\ bu_j \leftarrow db_i;\ j++;$
17. $Current = db_i; sz = 0;\ i++;$

else if $sz \geq 1$ then
$last = bu_j.pop()$; $BU \leftarrow bu_j$; $j++$; $bu_j \leftarrow last$;
$BU \leftarrow bu_j$; $j++$; $bu_j \leftarrow db_i$; $BU \leftarrow bu_j$; $j++$;
$Current = x$; $i++$; $sz = 0$;
else if
$Max = \max(Max, db_i)$; $Min = \min(Min, db_i)$;
if $|Max - Min| \leq TH_D$ and $sz \leq TB_S$ then
$bu_j \leftarrow db_i$; $Current = db_i$; $sz++$; $j++$;
else
$BU \leftarrow bu_j$; $Current = db_i$; $sz = 0$; $j++$;
end if
end while
return BU

2.2. Cluster-based Differential Data Method for data from diversified systems or devices

In this section cluster-based differential method is introduced and data is divided into subsets based on the similarity of the attributes with multi-dimensional properties received from the diversified devices of IoT applications. The similarity of the intent is strong in the intent scope. To differentiate the cluster centers the data is divided into heaps, so that the distance from the cluster centers to the clusters of the samples is minimized. K-means clustering algorithm is adopted to group the behavior of the clusters.

Consider the set of operations as intents containing $'n'$ data sources for an IoT application as $S = \{S_1, S_2, S_3, \ldots \ldots, S_i, \ldots \ldots, S_n\}$. Each data source contains $'m'$ features represented as $S_i = \{S_{i1}, S_{i2}, S_{i3}, \ldots \ldots, S_{im}\}$. The set is further divided into $'p'$ clusters as $S = \{cluster_1, cluster_2, cluster_3, \ldots \ldots, cluster_k\}$ and each cluster contains $'k'$ samples. $CL = \{CL_1, CL_2, CL_3, \ldots \ldots, CL_p\}$ be the cluster centers where $p < n$. The Euclidean distance between two points is calculated as follows:

$$d(S_i, S_j) = \sqrt{\sum (S_{ix} - S_{jx})^2} \qquad (1)$$

Where $i = 1, 2, \ldots \ldots, n$ and $x = 1, 2, \ldots \ldots, m$.

The sum of distances between the samples in the set divided by the total number of samples in the set is the average distance between the two points. Randomly set two samples from the set of samples. The average distance (AD) can be formulated as

$$AD = \frac{\sum_{i=1}^{n} \sum_{j=1}^{n} d(S_i, S_j)}{A_n^2} \qquad (2)$$

The density (DT) of the intent samples S_i is defined as: Let S_i be the center of the circle with the data objects and the number of objects in the circle is represented as $\propto * AD$, where be the coefficient adjustment of radius. If $d(S_i, S_j) \leq \propto * AD$ condition is true then the $cnt()$ function is cumulatively incremented by 1. 1 is the default value of the density of the intent sample.

$$DT(S_i) = \sum_{i=1}^{n} cnt(d(S_i, S_j) \leq \propto * AD) \ldots\ldots (3)$$

Where $i = 1, 2, \ldots\ldots, n$ and $j = 1, 2, \ldots\ldots, n$.

Further the average density (ADT) of the intent samples S is calculated as follows:

$$ADT = \frac{\sum_{i=1}^{n} DT(S_i)}{n} \ldots\ldots (4)$$

A collection of data objects whose density is a certain multiple of the average density of the intent sample set S is specified as high-density point set and defined as

$$HD = \{S_h\} \ldots\ldots (5)$$

Where S_h is a data object which belongs to dataset S which satisfy the condition $DT(S_h) \geq \beta * ADT$. β is the adjustment factor of density whose default value is 1.

The mean of sample set S is denoted as center of sample set S and represented as

$$S_{Center} = \frac{S}{n} \ldots\ldots (6)$$

The squared error sum (ERR) of the cluster is represented as

$$ERR = \sum_{i=1}^{a} \sum_{j=1}^{b} |S_{ij} - CL_i|^2 \ldots\ldots (7)$$

In the above equation, j^{th} data object of the i^{th} cluster is represented as S_{ij} and centre of i^{th} cluster is represented as CL_i

---

Algorithm: Cluster-based DP

Input: Meta-data from IoT applications ,

Output: IoT data based data for validating the differential privacy.

1. By using the equations (1 – 3) , Calculate the density of each object in the sample intent set S
2. Based on the equations (4 - 6) , Measure the high-density point set HD and also centre of intent sample set S_{Center}
3. According to the equation 6, compute the distance from HD to S_{Center} and select HD_i which satisfies the condition $\max(d(HD_i, S_{Center}))$ as the first cluster centre CL_1 to join the set CL;
4. repeat
5. Select the data object HD_j, if the condition $\max(d(HD_i, S_{Center}) * d(HD_i, CL_1))$ is true as the second initial cluster centre CL_2 is added to the set CL;
6. Until $|CL| = a$
7. Return metadata
8. //The centre of the cluster is selected
9. By distance, data objects are divided into the nearest cluster in the intent sample set S
10. As per the equation 7, compute the squared error sum (ERR) of the cluster and specify whether the union is converged
11. If the converges occurs, the clustering algorithms stops. Otherwise, previous step is executed again and the cluster centre is updated again
12. // Dividing the datasets

---

3. RESULTS AND DISCUSSION

This section explores the experimental study on the impact of differential privacy to validate the quality of the data using classification accuracy and test the scalability of the proposed methods to handle large multi-dimensional data. Comparison of the methods GenDP and cluster based algorithm has been done to validate the accuracy when the data is of homogeneous or partitioned into groups when it is heterogeneous using partition algorithm and in cluster based approach data is grouped into clusters based on the behavior and validate the data.

The proposed methods GenDP and Cluster based approach are applied on COVID-19 data set to evaluate the performance. To evaluate the classification efficiency in GenDP method with the partitioned algorithm, the data is divided into training and testing sets. Firstly , the algorithm is applied to evaluate the partitioning of the data in training phase and calculate the Ucuti. Later it was applied in GenDP to test the testing data for producing generalized test set and construct the classifier to measure the classification Accuracy (CA) on the generalized records of test data. In cluster-based approach the data is grouped based on the similarity and define the classifiers to evaluate the heterogeneous behavior of the data. The partitioning algorithm is used to group the data into different buckets or groups based on the behavior of the data. The number of partitions for homogeneous data is 1 and when the number of dimensions or volume of data increased the accuracy will be decreased.

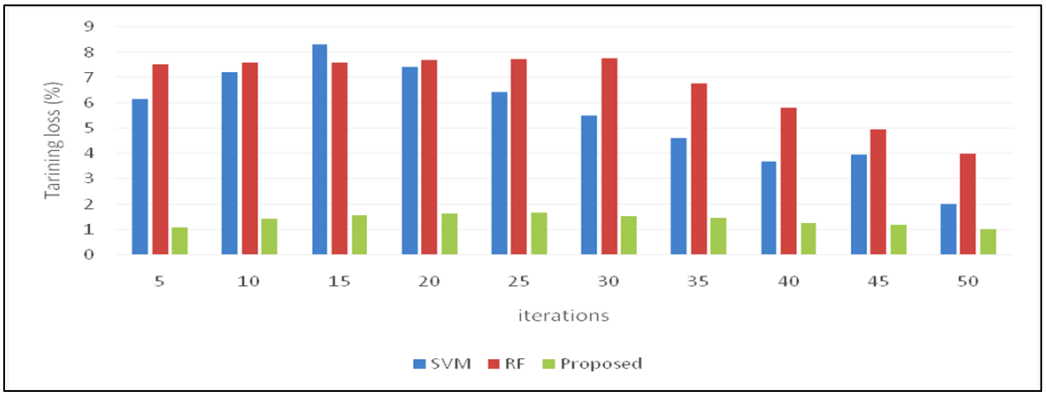

Figure 1. Training loss performance estimation.

Figure 1 presents the training loss performance estimation of various prediction model, where the proposed approach resulted in reduced loss performance as compared to Support Vector Machine (SVM) [15], Random Forest (RF) [16].Figure 2 presents the training accuracy performance estimation of various predication models, where the proposed approach resulted in increased performance as compared to SVM [15], RF [16].

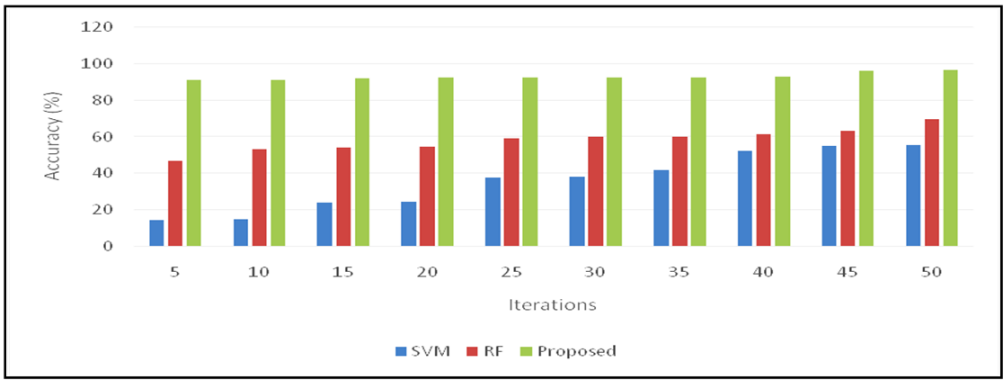

Figure 2. Accuracy performance estimation.

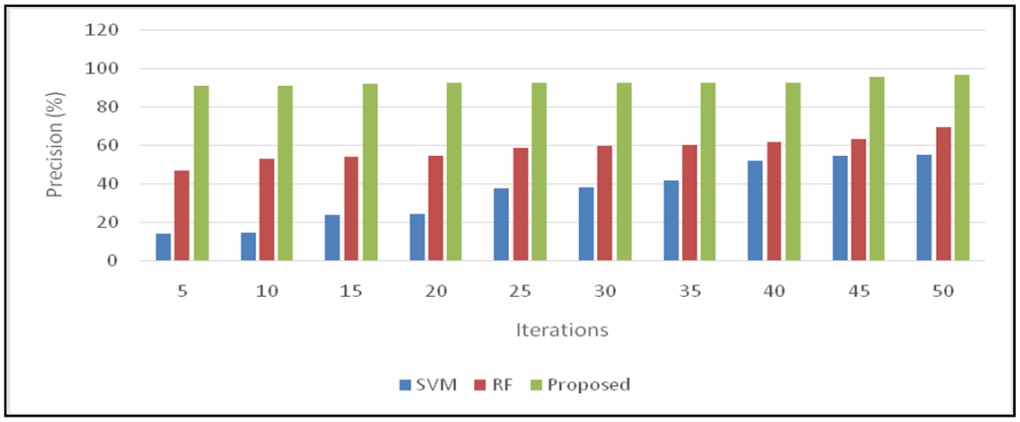

Figure 3. Precision performance estimation.

Figure 3 presents the precision performance estimation of various predication models, where the proposed approach resulted in increased performance as compared to SVM [15], RF [16].

4. CONCLUSION

This study defined two new algorithms for addressing the ε-differential privacy in large homogeneous or intents and heterogeneous data from diversified devices of IoT applications in Cloud computing domain. This algorithm classifies IoT meta-data and disseminated to the servers without revealing the sensitive information of the applications. The typical generalized DP algorithm explores the privacy in homogeneous and heterogeneous and defines the classifiers based the groups for validating the privacy and security policies. The clustering-based DP addresses the large multi-dimensional data and groups it based on the similarity for defining the classifiers to validate the ε-differential privacy. These methods maintain the good classification accuracy for various specifications and budget values of diversified intents and intent scopes.

REFERENCES

[1] M. Chamikara, P. Bertok, D. Liu, S. Camtepe, and I. Khalil, “An efficient and scalable privacy preserving algorithm for big data and data streams,” Computers & Security, vol. 87, p. 101570, 2019. https://doi.org/10.1016/j.cose.2019.101570

[2] Security- and privacy-aware IoT application placement and user assignment.Zolt´anAd´am Mann.Computer Security — ESORICS 2021 International Workshops, Lecture Notes in Computer

Science, vol. 13106, Springer, pp. 296-316, 2022.https://www.cs.bme.hu/~mann/publications/ESORICSW-2021/Mann_ESORICSW_2021.pdf

[3] Privacy and Security in IOT Cloud-Based Healthcare System. Deepika Dhawan and Faiyaz Ahmad.Volume-12, Issue-3 (June 2022).International Journal of Engineering and Management Research https://doi.org/10.31033/ijemr.12.3.7

[4] Linyuan Liu, Haibin Zhu, Shenglei Chen, Zhiqiu Huang, "Privacy-Aware Task Assignment for IoT Audit Applications on Collaborative Edge Devices", Security and Communication Networks, vol. 2022, Article ID 1336094, 15 pages, 2022. https://doi.org/10.1155/2022/1336094

[5] Corno, F., De Russis, L. &Mannella, L. Helping novice developers harness security issues in cloud-IoT systems. J Reliable Intell Environ **8**, 261–283 (2022). https://doi.org/10.1007/s40860-022-00175-4

[6] I. Roy, S. T. V. Setty, A. Kilzer, V. Shmatikov, and E. Witchel. Airavat: Security and privacy for mapreduce. In NSDI, pages 297–312. USENIX Association, 2020. DOI: 10.4236/jis.2020.114019

[7] Yang G. An Overview of Current Solutions for Privacy in the Internet of Things. Front ArtifIntell. 2022 Mar 3;5:812732. doi: 10.3389/frai.2022.812732. PMID: 35310954; PMCID: PMC8928167.

[8] Yang G. (2022). An Overview of Current Solutions for Privacy in the Internet of Things. Frontiers in Artificial Intelligence. 5:812732. https://doi.org/10.3389/frai.2022.812732

[9] Jörg Christian Kirchhof, Bernhard Rumpe, David Schmalzing and Andreas Wortmann. (2022). MontiThings: Model-driven Development and Deployment of Reliable IoT Applications. In: Journal of Systems and Software (JSS).183. 111087, Elsevier. www.se-rwth.de/publications/

[10] Bindschaedler, V., Shokri, R., & Gunter, C. A. (2016). Plausible deniability for privacy-preserving data synthesis. Proceedings of the VLDB Endowment, 10(5), 481-492. https://doi.org/10.14778/3055540.3055542

[11] S. Su, P. Tang, X. Cheng, R. Chen and Z. Wu, "Differentially private multi-party high-dimensional data publishing," in Proceedings of IEEE 32nd International Conference on Data Engineering (ICDE) ,2016, pp. 205-216.

[12] Fortino, G.; Guerrieri, A.; Pace, P.; Savaglio, C.; Spezzano, G. IoT Platforms and Security: An Analysis of the Leading Industrial/Commercial Solutions. *Sensors* **2022**, *22*, 2196. https://doi.org/10.3390/s22062196

[13] M. Usman, M. A. Jan, X. He and J. Chen, "P2DCA: A Privacy-Preserving-Based Data Collection and Analysis Framework for IoMT Applications," in IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1222-1230, June 2019, doi: 10.1109/JSAC.2019.2904349. https:// 10.1109/JSAC.2019.2904349

[14] Qian, H., Li, J., Zhang, Y. et al. Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation. Int. J. Inf. Secur. 14, 487–497 (2015). https://doi.org/10.1007/s10207-014-0270-9

[15] J.Deepika,C.Rajan,T.Senthil, " Security and Privacy of Cloud- and IoT-Based Medical Image Diagnosis Using Fuzzy Convolutional Neural Network",Journal of Computaional Intelligence and Neuroscience, vol.2021, https://doi.org/10.1155/2021/6615411

[16] Shankhpal, SV, SavadattiHanumantha, B. KMFA2 based QoS improvement for multi-channel IoT networks. *Concurrency ComputatPractExper*. 2022; 34(15):e6949. doi:10.1002/cpe.6949

AUTHORS

Dr Subba Reddy Borra received the B.Tech from Bapatla Engineering College. M.Tech obtained from JNTUK in Specialization Neural Networks. Received Ph.D from JNTUH in 2021. I have 22 Years of experience and working as Professor and Head in Department of Information Technology from Malla Reddy Engineering College for Women (UGC-Autonomous) ,Hyderabad,India..My area of interest is Image Processing and Machine learning.

Dr. SMITA KHOND is currently working as Associate Professor in IT Department in Malla Reddy Engineering College for Women, Hyderabad since 2011 and Ratified by JNTU Hyderabad. She received her B. E (CSE) from Dr. Babasaheb Ambedkar Marathwada University Maharashtra, M. TECH (CSE) from G.H. Raisoni Engineering College Nagpur and Ph.D. (CSE) from Pacific University, Udaipur. She has qualified GATE exam with 88 percentile score. And her area of interests are Image Processing, Cloud Computing and Network Security. Dr. Smita is having 15 years of experience in Teaching and 4 years of experience in Research. She has published more than 10 papers in various international journals and conferences. Also attended various FDPs, Workshops and Training programs. She has done more than 20 Coursera certifications

D. Srivalli is currently working as an Assistant Professor in IT Department in Malla Reddy Engineering College for Women, Hyderabad since 2017 and Ratified by JNTU Hyderabad. She received her B.Tech (IT) from JNTU,Hyderabad. M. TECH (SE) from JNTU, Hyderabad.And her area of interests are Data Mining, Cloud Computing and Network Security. D.Srivalli is having 8 years of experience in Teaching. She has published more than 5 papers in various international journals and conferences. Also attended various FDPs, Workshops and Training programs. She has done more than 10 Coursera certifications