**Improving Cloud Privacy and Confidentiality Using Enhanced DNN Architecture on Laplace Mechanism (Laplace Gaussian exponential)**

*Richard Okumali*

*Department of Computer Science and Technology*

*Donghua University*

[*richardokumali@gmail.com*](mailto:richardokumali@gmail.com)

**Abstract**

***Privacy and confidentiality of data and information on cloud storage platforms is critical and a major area of concern. Cloud-based security measures, end-user encryption systems, and training and awareness programs on data and information security have been used to improve data confidentiality. However, these measures need to be sufficient and effective to realize the confidentiality and privacy of data and information. In this regard, we implement a joint LGE (Laplace Gaussian exponential) mechanism to achieve the goal of confidentiality and privacy. The approach increases noise on data, thus masking details on data deemed private and confidential***.

**Introduction**

T

he privacy and confidentiality of data and information is significant when debating data and information security. Cloud privacy and confidentiality, or the concept of keeping the cloud secure, is a challenge that experts are concerned about. While companies and organizations continue to migrate to the cloud, the puzzle around confidentiality remains unsolved. Experts' analysis has indicated that distributed systems, an architecture of cloud-based systems superimposed on clients, expose data and information to vulnerabilities. In other words, the ability to access data from multiple geographical locations makes it easier for malicious individuals to perpetrate data stores and achieve their goals illegally.

The main problem with cloud-based systems is achieving reliable security (privacy and confidentiality) to assure end users of maximum privacy and confidentiality. Other experts in the field might argue that there exist measures already implemented and some still in implementation that would help improve security. The core problem, however, is different from the measures. The question which also forms the problem is: are these measures authentic and definitive? In a report and research on cloud-trust mechanisms, advanced and persistent threats have been cited as a concern to governments and industry. Many institutions need to be more suspicious of the authenticity of data and security controls that cloud computing companies have already implemented.

**The Problem**

A lot has already been done at different levels. Some cloud computing companies have left third-party companies to handle all data and information security protocols and measures. Others have clarified that end users are responsible for the security of all data and information stored on the cloud [1]. While assessing the entire problem, questions might arise on the possible aspects behind the security issues. Ideally, data is a resource for decision-making, analysis, and forecasting, among many other activities [2]. According to Harkut [2], data forms the backbone of any upcoming, existing, future, and successful institution or business. Data has value to any business or organization, a concept that competitors, hackers, and other stakeholders in the dataspace understand best. Upon knowing the value, many would be in the race to acquire more data legally or illegally for various uses.

T-Mobile, a US–based mobile and Internet Service Provider (ISP), reported a data breach in early May 2023. The breach into the company's cloud server revealed the personal identification numbers (PINs), full names, and mobile phone numbers of over 800 customers in early May 2023 [3]. Despite the layered security measures put in place in some cloud computing solutions, reports on data leaks have significantly increased. Multi-factor authentication, also known as duo-push, password-less authentication, port view for all devices, and a zero-trust network access approach, are countermeasures. In addition to other sophisticated solutions, organizations focus on educating and creating awareness as a mitigation measure to enhance data and information at an organizational and cloud level. However, The bottom line is that these measures are unreliable, implying that the possibility of malicious access to data and information is still high.

Scalability, rapid elasticity, multi-latency, service, and resource, among other qualities of the cloud, must be maintained when implementing any improvements. Therefore, when considering the implementation of any cloud improvements, these aspects must be put into consideration. Instead of reducing them, improvements must either strengthen or increase performance for the benefit of the end users. Upon having all the facts right, we focus on strengthening the lapse mechanism – a technique used in differential privacy to add noise to datasets before they are analyzed. In this case, the dataset includes end-user data and information stored in the cloud. At its core, the lapse mechanism is implemented in cloud computing to achieve differential privacy because of its unique characteristics and capabilities of allowing large-scale data processing and storage.

**Literature Review.**

Governments and the entire information technology industry are concerned with the persistent threat of private and confidential data breaches. To solve the problem, Gonzales [4] recommends a cloud-trust model which incorporates an array of security controls and best practices in estimating low- and high-level security requirements and metrics of confidentiality. The cold trust model runs on the cloud's infrastructure as a service level (IaaS). The model assesses the security of four major levels of the IaaS, which also have alternative security measures and protocols. In the study, the model effectively handles disk injection-related attacks, live VM, and areas associated with undetected configuration modification. While the cloud-trust model proved efficient, Gonzales [4] mentioned that it failed to include all possible insider attack vectors and methods. The approach is also limited to IaaS, cloud service providers (CSP), and cloud computing systems (CCSs) [5]

HoneyNets have also been recommended and used to achieve a similar solution. According to Eric and Toth [6], cloud-based security is essential for the success of businesses and operations that depend on it. As a result, Eric and Toth [6] recommend a software-defined network security-based approach whose role is to frameworks that would help secure cloud IoT. The proposed solution implements an end-to-end security assessment approach based on software-defined networking (SDN) to achieve the evaluation process. The goal is to ease the implementation of network controls at different levels of the cloud system. The SDN system develops a three-layer system of 23 indicators describing essential security features. Though helpful and realistic, the approach fails to present a technical solution to security issues and challenges affecting cloud-based systems. Eric and Toth [6] state that future studies should consider expanding the interview scope to better understand the scope and depth of cloud – IoT systems to achieve a comprehensive solution.

Khaled Chait [7]implements a partially homomorphic multi-key-based additive encryption system on cloud data and storage to secure cloud data and information. Homeomorphs allow end-users and stakeholders (third-party individuals) to access data without having access to it [7]. Previous research results have shown that most encryption systems' case access to data and information becomes slower through increasing execution time. These challenges are contrary to the emerging trends in cloud computing and the ever-increasing business needs. Test results multi-key homomorphic key-based additive encryption system showed a high level of hardness and efficiency [7]. A deeper analysis of the results and conclusions made by Khaled, however, reveals that the model works effectively on low computing capacity devices, leaving out a wide range of high-capacity devices that characterize the new day cloud – IoT system.

Artificial Intelligence (AI) and machine learning concepts have revolutionized computing and cloud computing in various ways. While considering the privacy and confidentiality of cloud-based systems, Vikas [8] implements AI-assisted security controls to map end-user security needs, eliminating the current manual process implemented by many cloud-based providers. The AI model marks the beginning of a new dawn in configuration and determines the security demands of end users. However, it needs to address the critical question of reliability, accuracy, and strength of the security solutions that would be implemented. Ideally, Vikas [8] has left a gap that requires experts to conduct further research, tests, and analyses and ensure a secure and seamless flow of end-user data and information.

Other strategies employed to achieve security, particularly data privacy and confidentiality, include the use of blockchain and LDP-based smart healthcare IoT [9]. Combined, the strategies have helped secure cloud-based data and operations at different levels. On the contrary, AI and machine learning solutions have yet to be explored in-depth. Artificial Intelligence and the field of machine learning are emerging giants in the technological domain. Considering their abilities and leveraging their availability will usher in a new way of conducting operations on cloud computing and other related domains like IoT.

**Enhanced DNN Architecture on Laplace Mechanism**

1. Laplace Mechanism

The Laplace mechanism serves the purpose of adding noise to data to satisfy differential privacy [1]. Differential privacy is a technique used in cloud computing to protect sensitive data while allowing end users to access and use it for analyses [1]. The approach adds noise to data, making it difficult to identify individual records. Given a dataset X with a sensitivity degree S and a privacy parameter epsilon, the Laplace mechanism would add noise as in the formula.

Epsilon is a term or a metric of privacy loss at a differential change in data. In the epsilon technique, the smaller the value, the better the privacy protection. Ideally, a lower epsilon lowers the impact of individual data and aggregated results and further increases privacy while reducing redundancy. The scale parameter in the above formula controls the amount of noise added to the data. Larger scale values would correspond to more noise and else otherwise.

1. Combined LGE mechanism

The combined LGE mechanism adds multiple types of noise to a given dataset - Laplace, Gaussian, and Exponential. For instance, on a given dataset X with sensitivity S with the following parameters, *epsilon\_laplace, epsilon\_gaussian, epsilon\_exponential,* and *delta,* the LGE mechanism will work as follows.

The Laplace (scale = S/epsilon\_laplace) denotes the random variable drawn from the Laplace distribution with a 0 – mean.

The scale S/epsilon\_laplace, denotes random variables from a Gaussian distribution with also an average of 0 and standard deviation of .

The Exponential ) denotes variables drawn from the exponential scale with smaller data values corresponding to stronger privacy guarantees.

*Note that the specific formula for the LGE mechanism may vary depending on the particular implementation and choice of noise distributions. The formula provided here is based on the formulation proposed by Dwork et al. in their paper "Exponential Mechanisms for Local Differential Privacy."*

**Results**

Using test data, the following are the results of our LGE model for achieving differential privacy in cloud datasets.

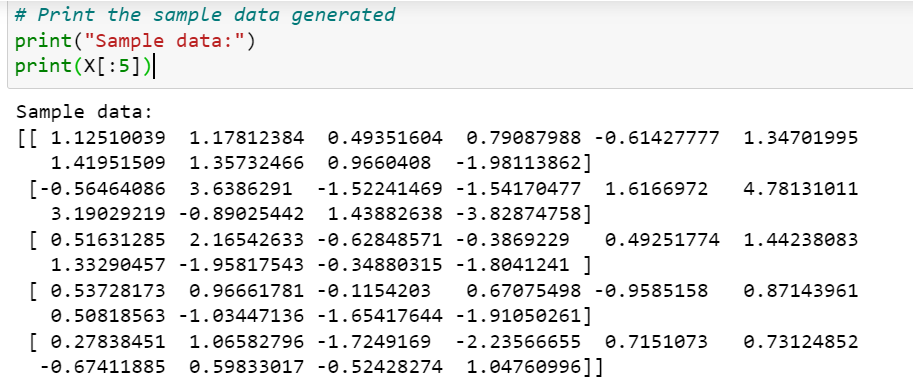


Figure 1: Generated Sample Data

A picture containing text, screenshot, line, plot

Description automatically generated

Figure 2: Accuracy Comparison

From the graph, our LGE mode effectively added noise to the provided sample dataset. The accuracy significantly reduced after the whole process. The results imply that critical information about the data has been achieved, and critical information about individuals or companies has been masked successfully.

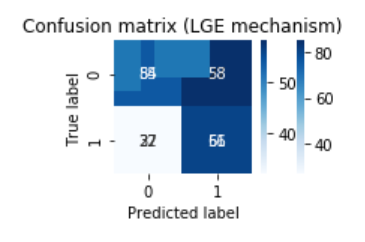


Figure 3: Confusion Matrix on LGE Implementation

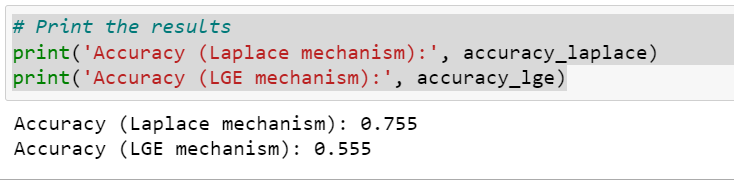


Figure 4: Further Results

Further results on LGE mechanism. The accuracy level of the Laplace mechanism alone is at 75%. However, when LGE is used, the accuracy falls to 55%, implying a 20% drop in accuracy—the less accurate the data, the more accurate the confidentiality and else otherwise.

**Limitations**

When considering such an approach in realizing differential privacy, concerns about trade-offs between privacy and utility are common. According to Han [5], increasing the privacy levels of data can have a significant impact on the utility of the data. The model used to realize differential privacy implements logistic regression on the data. It is, however, essential to understand that the data used in this case is sample data. In other words, different datasets would require different models because of different parameters. We can, therefore, only conclude that the mode is efficient in all datasets if otherwise. And these doubts leave us in limbo, given that some datasets are prone to overfitting or underfitting depending on the data provided. Considering these limitations when implementing the model in a real cloud environment might give better results.

Further research should also consider finding methods and measures that can help increase processing speed. The mode adds more noise to data, thus increasing privacy and confidentiality. However, these changes make it challenging to analyze the data and revert it to normal when needed. The reverse process might require a lot of processing resources, which is a major drawback when implementing it.

**Conclusion**

The LGE mechanism achieved differential privacy by adding Laplace, Gaussian, and Exponential noise to cloud data. The whole concept aims to improve privacy protection by combining three models or approaches. However, challenges related to the LGE mechanism must be overcome to be effective and efficient enough. Its complexity makes it challenging to optimize and implement. The choice of epsilon values and the parameters that help achieve privacy protection and different noise distributions vary from dataset to dataset. As a result, if the parameters are not well analyzed, they can compromise the data's utility and the model's overall accuracy.

The mechanism also involves trade-offs between privacy and the utility of data. In other words, increasing the levels of privacy can significantly impact the accuracy of the model. These challenges call for precision and detail when choosing privacy parameters and evaluating trade-offs between privacy and utility in specific use cases. The LGE mechanism is a promising approach that can help preserve privacy in cloud data storage systems. Still, it requires careful implementation and evaluation aimed at achieving a balance between privacy and the protection of the quality of data and information.

**References**

[1] S. A. N Holohan, S Braghin, "The bounded Laplace mechanism in differential privacy," *Journal of Privacy and Confidentiality,* 2020, doi: 10.29012/jpc.715.

[2] G. Harkut, "Introductory chapter: Cloud computing security challenges," *Cloud Computing Security - Concepts and Practice,* 2020, doi: 10.5772/intechopen.92544.

[3] D. Goodin. "T-Mobile discloses 2nd data breach of 2023, this one leaking account PINs and more." <https://arstechnica.com/information-technology/2023/05/t-mobile-discloses-2nd-data-breach-of-2023-this-one-leaking-account-pins-and-more/> (accessed.

[4] D. Gonzales, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," 2020.

[5] K. H. Zhuobing Han, "A Software Defined Network-Based Security Assessment Framework for CloudIoT," *IEEE Internet of Things Journal,* 2019.

[6] M. C. Eric M Toth, "Honeynets and Cloud Security," 2022.

[7] A. L. Khaled Chait, Lamri Laouamer, Mostefa Kara, "A Multi-Key Based Lightweight Additive Homomorphic Encryption Scheme," 2021.

[8] R. B.-H. Vikas Agarwal, Lilach Eden, Nisha Gupta, Yoav Kantor, Arun Kumar∗, "AI-Assisted Security Controls Mapping for Clouds Built for Regulated Workloads," *IEEE 14th International Conference on Cloud Computing (CLOUD),* 2021.

[9] F. A. Maham Iftikhar, "Blockchain and LDP-Based Smart

Healthcare IoT Applications," *Architecture, Challenges and Future Works,* 2023.