**The Effects of Privacy Protection on Forecast Accuracy**

**Introduction**

1. Sensitive time series are highly useful in many fields but come with privacy risks.
   1. Consumer Analytics – requires sensitive consumer-level data.
      1. Forecasting consumer behavior can help improve demand forecasts and supply chain efficiency (Boone et al., 2019). However, this often requires data linked to consumer identities. One example is credit card reports, which can be used to easily identify individuals even after direct identifiers such as names and account numbers are removed (de Montjoye et al., 2015).
      2. Consumer health data can be used to provide real-time health monitoring, help achieve fitness goals, and provide disease diagnostics, but is also subject to privacy concerns (Imtiaz et al., 2020).
      3. User generated content can be used to forecast individual health outcomes (Reece et al., 2017), and has been shown to help reduce forecast errors when models are supplemented with UGC data. However, even content posted anonymously online can present a risk of re-identification to the author (Schneider & Mankad, 2021).
   2. Energy forecasting – requires commercially or personally sensitive data.
      1. Renewable energy forecasting accuracy can improve when data owners collaborate and share data, but data owners often won’t share their data due to privacy concerns (Goncalves, Bessa, et al., 2021; Goncalves, Pinson, et al., 2021; Sommer et al., 2021).
      2. Smart meter data enables utility companies to bill customers more accurately and enables customers to have better insight into their energy usage. This smart meter data has many privacy risks including revealing occupancy and activity patterns or enabling discriminative business practices (Véliz & Grunewald, 2018).
   3. Census data – aggregate data is derived from sensitive information on individuals and businesses.
      1. Quarterly workforce indicators data provides useful longitudinal information such as wages, job creation rates, and hiring levels across various groups such as age, race, and education. An example use case is forecasting productivity growth in the U.S. economy (Ozimek et al., 2018).
2. Why privacy risks need to be addressed.
3. How privacy risks can be addressed while maintaining data usefulness.
   1. Data use agreements stipulate when and how data can be used. These are common whenever data is shared between parties, but alone offer little protection against data breaches or attacks against sensitive data.
   2. Distributed learning enables computations to be performed at the source of the data (e.g., on the edge) which means sensitive data does not need to be transferred. These solutions are suitable when all parties have sufficient computational power and the models that are being trained are separable.
   3. In many instances, data is stored by a single data provider who shares that data with interested parties. The data privacy literature offers a wide array of solutions to the problem of protecting the identities and attributes in a dataset.
   4. Data privacy law supports the notion that data can be anonymized and shared with other parties with significantly less risk to data subjects.
4. The implications of data protection for the forecasting community.
   1. Forecasters have difficulty obtaining access to sensitive data at the granularity they need (Matt may have examples of this).
   2. However, only a few papers have examined how data protection can be applied to time series, and how this protection affects common uses of time series data (Abowd et al., 2012; Nin & Torra, 2009).
   3. There is also very little work that compares the accuracy of time series models applied to protected data (Gonçalves et al., 2021).
   4. If forecasters wish to obtain access to sensitive data that is otherwise unavailable, data protection techniques may be the most viable route for data providers to meet the demand for data while protecting data subjects.
   5. Even though privacy law supports data anonymization and there are a wide variety of anonymization techniques to choose from, the forecasting community has not given in-depth exploration to the interaction between data privacy and forecasting. This is the gap we seek to address.
   6. We wish to address the following research questions:
      1. How do the accuracies of popular forecasting models change under data protection?
      2. What time series and model characteristics drive these changes?
      3. Does data protection always reduce forecast accuracy? Or do certain combinations of protection methods and forecasting models lead to improved accuracy *and* improved privacy?
      4. Given a data protection method, which forecasting model produces the best accuracy?
      5. Can we design a new time series protection method that offers a more favorable trade-off between privacy protection and forecast accuracy than existing protection methods?
5. Focus of this paper.
   1. Compare the accuracies of forecasting models under various data protection methods applied to a dataset (classic data sharing – not distributed).
   2. Understand how data protection alters time series characteristics and leads to information loss (or gain) that changes forecastability.
   3. Guide forecasters on selecting a forecasting model, given data characteristics and a protection method.

**Literature Review and Hypotheses**

1. Existing work on data privacy and forecasting.
   1. (Goncalves, Pinson, et al., 2021) explore a data market scenario in which data owners are compensated to share their own data, and purchase forecasts based on the data from other parties. In this scenario, data owners have a monetary incentive to share their data, but may be discouraged from doing so due to privacy concerns over sharing data with a central party. Our work would help answer how forecast accuracy would be affected if the data owners applied data protection methods prior to sharing their data.
   2. Transfer learning (Wellens et al., 2021) is mainly designed to reduce the computational burden of training complicated machine learning (or deep learning) models from scratch. An added benefit is that these models could be trained on sensitive data and transferred themselves, without transferring the sensitive data. While transfer learning can overcome privacy barriers or regulations, forecasting using shared, protected data, not shared models, is the focus of our paper. We care about how multiple forecasting models, from simple to complex, perform when trained on protected data.
   3. (Gonçalves et al., 2021) explored methods for preserving data privacy in the context of collaborative forecasting. The methods they explored were broken into three categories: data transformation, secure multi-party computation, and decomposition-based methods.
   4. Secure multi-party computation was found to be very computationally expensive without fully preserving privacy when forecasting using a VAR model. Our goal is to understand forecasting under less computationally demanding protection methods which are more commonly used. Moreover, we consider a single protected dataset, rather than a collection of smaller datasets across multiple parties.
   5. Decomposition based methods are based on an iterative process that can reveal sensitive data to the participating parties and the central node after multiple iterations. (Sommer et al., 2021) added an encryption matrix to their protocol which would prevent the competing parties, but not the central node, from recovering sensitive data. A remedy to this was proposed by (Goncalves, Bessa, et al., 2021), who added a data transformation step to their distributed learning algorithm, enabling privacy-preserving collaborative forecasting without reductions in forecast accuracy. Our interest is in forecasting using a single protected dataset, and the proposed decomposition methods are not easily extendable to complicated non-linear models, such as LSTM neural networks, which we will use in our study.
   6. The final area explored by (Gonçalves et al., 2021) is data transformation techniques – their chosen technique, differential privacy, involves a direct trade-off between privacy and forecast accuracy. Even very high values of the privacy parameter (low privacy) result in reductions in forecast accuracy for VAR models. In the literature, differential privacy is the most popular data protection method applied to time series, see (Imtiaz et al., 2020; Liyue Fan & Li Xiong, 2014) for examples. An interesting result from (Imtiaz et al., 2020) is that differentially privacy data did not always produce worse forecast accuracy when forecasting individuals’ health data using a recurrent neural network. Since adding random Gaussian noise to time series is a technique to prevent overfitting when forecasting with neural networks (Hewamalage et al., 2021), we will explore whether data protection can achieve this same effect and improve forecast accuracy for neural networks. However, even if this occurs, we expect it only for very high values of epsilon, which may not correspond to meaningful levels of privacy.
   7. Other data transformation techniques:
      1. Additive/Multiplicative noise is similar to differential privacy in that random noise is infused into the data, but there are no theoretical privacy guarantees with this version of protection. Example applications include (Abowd et al., 2012), who discuss the Census’ use of multiplicative random noise to perturb the individual or business level data that goes into calculating Quarterly Workforce Indicator data – but they do not assess the accuracy of forecasting with the perturbed data. More recently, (Luo et al., 2018) use multiplicative random noise to simulate a data integrity attack in the context of load forecasting. They measure the accuracies of multiple linear regression, artificial neural network, support vector regression, and fuzzy interaction regression models on the original and attacked data. The authors found the while multiple linear regression performed the best on the original data, the support vector regression was most robust and performed the best under the data integrity attacks – we expect similar findings in our work, where the best models on the original data will not necessarily be those that perform the best on protected data. An important note is that the integrity attacks did not affect every data point in the series – significant reductions in accuracy occurred when just 40% of the points in a series were altered by a large magnitude. If differential privacy or additive/multiplicative random noise are used to add significant amounts of random noise, we expect massive reductions in accuracy since every point in the time series will be altered.
      2. *K*-anonymity is a principle describing when every record (or time series) in a dataset is identical to at least *k*-1 other records. It was originally proposed by (Sweeney, 2002). Similar to our work, (Nin & Torra, 2009) evaluate the change in forecast accuracies of simple exponential smoothing, double exponential smoothing, linear regression, multiple linear regression, and polynomial regression applied to *k*-anonymized data. While they find significant reductions in forecast accuracy across all five models even for *k*=2, they do not provide a comparison between models or additional data protection methods.
      3. The final protection method we review is top and bottom coding. An example use case for bottom coding would be to prevent inferring when homes are empty from smart meter data by setting all measurements below the th quantile equal to the th quantile. (Crimi & Eddy, 2014) study the effect of top coding the Census’ Public Use Microdata Samples on analyses of interest. They find that the sample correlation between two variables is shrunk towards zero when one or both of the variables are top coded. Extrapolating this to our scenario, multivariate forecasting model performance, which relies heavily on the correlations between time series, may be negatively affected when all series are top or bottom coded.
   8. Gaps in Existing Work on Data Privacy and Forecasting
      1. While recent attention has been paid to privacy-preserving collaborative forecasting, there has been no work to compare multiple forecasting models’ accuracies when forecasting for a single protected dataset of multiple time series, or a comparison of these models’ accuracies under different forms of data protection. There are unanswered questions that result, such as, does every combination of data protection method and forecasting model result in a reduction in forecast accuracy? Given that my data has been protected, which forecasting model should I choose?
      2. The works which show reductions in forecast accuracy for a VAR model applied to differentially private data (Gonçalves et al., 2021), or multiple forecasting models under data integrity attacks (Luo et al., 2018), did not explore the underlying reasons *why* the forecast accuracy changed – this leaves open questions such as, how are time series characteristics like seasonality or trend affected by data protection? How do these effects translate into variation in the performance of forecasting models meant to model these characteristics? In addition, not only will data protection result in changes to the data, it will produce changes to the forecasts themselves. How do the changes in forecasts translate into changes in forecasting model performance? Can we explain changes in performance using the direction or magnitude of the changes in forecasts?
2. There is a judgmental forecasting literature examining how model based forecasts are adjusted by practitioners to increase (or sometimes damage) forecast accuracy – see (Petropoulos et al., 2022) for a summary.
3. Informed by findings from judgmental forecasting literature, we will examine the changes in forecast accuracy through two lenses: (1) how changes to time series characteristics translate to changes in forecast accuracy; and (2) how changes to the forecasts themselves affect forecast accuracy.
   * 1. How changes to time series translate to changes in forecast accuracy.
        1. Judgmental adjustments can increase accuracy when based on reliable information, but information with low diagnosticity can damage forecast accuracy (Fildes et al., 2009, 2019). When accuracy did improve, increases in accuracy from adjustments to forecasts were greater for low volatility series which are easier to forecast (Fildes et al., 2009). It was also discovered that forecasters tended to make unnecessary adjustments to model-based forecasts which damaged accuracy.
        2. We expect random noise protection (differential privacy and additive/multiplicative noise) will increase time series’ volatility and will add “information” with no diagnosticity, thereby adjusting the forecasted values – based on the findings stated previously, this would mean the adjustments to forecasts from these protection methods will, in general, damage forecast accuracy, as has already been demonstrated for VAR models and recurrent neural networks (Gonçalves et al., 2021; Imtiaz et al., 2020). However, we will examine whether small amounts of random noise protection serve as regularization for recurrent neural networks and end up improving accuracy.
        3. On the other hand, top and bottom coding should reduce volatility. Moreover, adjusting for outliers, mainly those close to the forecast origin, can increase forecast accuracy (Chen & Liu, 1993). We expect that for moderate amounts of top/bottom coding, we will see an improvement in forecast accuracy for series that are more volatile and/or have outliers near the forecast origin.
     2. How changes to forecasts translate into changes in forecast accuracy.
        1. Direction of adjustment.
           1. Both negative and positive adjustments increase accuracy (positive gives only marginal increase), overall accuracy increased by 10% (Davydenko & Fildes, 2013). Negative adjustments tended to reduce bias, while positive adjustments maintained bias magnitude or exacerbated it (Fildes et al., 2009).
           2. For judgmental forecasts, the direction of adjustment is chosen with the intent of improving the forecast – under data protection, direction is a result of the protection method, without regard to the effect on forecasts. Adjustment direction will be random under random noise protection, but top (bottom) coding will likely adjust the majority of forecasts downward (upward). Based on the previous findings, we expect that top coding will have a more significant improvement on forecast accuracy than bottom coding. We will also examine whether any observed increase (damage) in forecast accuracy is a result of a reduction (increase) in forecast bias.
        2. Size of adjustment.
           1. (Fildes et al., 2009) found that the size of adjustments was positively associated with the size of accuracy improvements. One explanation given is that an adjuster who is more confident will make a larger adjustment, which improves accuracy when based on reliable information.
           2. Under data protection, the adjustment size will be determined by the forecasting models’ responses to changes in the data, where the size of changes in the data will be governed by the strength of the data protection.
           3. Strength of protection is determined by the magnitude of noise (random noise protection) or the percentage of top/bottom coded observations.
           4. Large amounts of random noise or top/bottom coding will produce significant perturbations in the data which will likely lead to large adjustments in forecasts. We expect the size of adjustment to be negatively related to changes in accuracy under random noise protection. However, large adjustments in forecasts could occur under top/bottom coded data if a large outlier is adjusted near the forecast origin. So, we expect a positive relationship between adjustment size and changes in accuracy for small percentages of top/bottom coding, and a negative relationship between adjustment size and changes in accuracy for large percentages.
4. Our contributions.
   1. An extensive comparison of forecasting models’ accuracies on protected data.
   2. Explanation of how data protection alters time series characteristics *and* forecasts, and how these changes translate into changes in forecast accuracy.
   3. Past work offers suggestions for improving accuracy of judgmental forecasts (Alvarado-Valencia et al., 2017; Fildes et al., 2009) – to do this for forecasts based on protected data, we must first understand how forecasts are affected by data protection.
   4. Discuss how our results inform managerial decisions for forecasting using protected data.

**Experimental Design**

1. Overall Forecasting Framework.
   1. Obtain original series
   2. Create protected series
   3. Extract time series characteristics from and
   4. Train each forecasting model on and
   5. Generate forecasts for and
   6. Compare forecasts and time series characteristics from and
      1. Accuracy measures.
      2. Examine changes in time series characteristics and adjustments to forecasts to explain model performance.
2. Data – M3 monthly Micro
   1. Machine learning models perform well.
   2. Models that explicitly model trend and seasonality performed the best (Kang et al., 2017), so we examine how changes in these features affect the accuracy of these models.
   3. Provides a reasonably high number of series (474).
   4. Relates to business (commercially sensitive?) data which may require protection.
3. Treatments
   1. Methods
      1. Differential privacy, top/bottom coding, additive/multiplicative noise
   2. Parameters to vary
      1. Level of protection (, % top/bottom coded, etc.)
4. Explaining forecasting model performance.
   1. Extract time series features and visualize using instance space (PCA applied to extracted features) (Hewamalage et al., 2022; Kang et al., 2017).
      1. Spectral entropy (forecastability/diagnosticity).
      2. Coefficient of variation (directly measure volatility) (Fildes et al., 2009).
      3. Strength of trend and seasonality.
      4. First order autocorrelation.
      5. Optimal box-cox transformation parameter.
5. Selection of Forecasting Models
   1. Popular models found in R, Python and/or serving as benchmarks in forecasting competitions. These models show how forecast accuracy would change for ‘non-expert’ users.
      1. SES, DES, TES, ARIMA, Prophet (Facebook), Greykite (LinkedIn), LGBM (univariate), VAR.
      2. Perform minimal data pre-processing
         1. Log transform – removes multiplicative effects and stabilizes variance – improves model convergence.
         2. Convert to stationary series (ARIMA)
         3. Allow the models to capture the important aspects of the time series.
   2. Cutting-edge multivariate models.
      1. LGBM (multivariate) (Hewamalage et al., 2022)
         1. Direct modeling (train one model for every horizon step).
         2. MAE as loss function.
         3. To avoid overfitting: early stopping mechanism when validation error does not improve over 5 consecutive epochs.
         4. Max epochs and learning rate set to 1200 and 0.075.
         5. Range blending (Lainder & Wolfinger, 2022).
         6. Clustering (Hewamalage et al., 2022).
      2. NeuralProphet
      3. RNN (LSTM cells)
      4. Perform pre-processing that is consistent with best practice – what “should” be done - (outline exact steps in appendix).
   3. Hyper-parameter tuning
      1. For ‘non-expert’ models
         1. Expanding window cross-validation – easily performed in Python library sktime, described in (Lainder & Wolfinger, 2022)
            1. Split data into train, test (where test is the length of the forecast horizon)
            2. Set initial window length to 70% of available training data.
            3. For each hyperparameter combination in grid:

While horizon does not equal last available training data:

Train model on current window of training data

Evaluate forecast accuracy (MAE) on the horizon following the current training data window.

Expand window forward one step and repeat.

* + - 1. Train model on the full training data using the optimal hyper-parameters (determined by mean MAE across folds)
      2. Evaluate model on the test data (MAE).
    1. For cutting edge models
       1. LGBM
          1. While valid to use standard *k*-folds CV (Bergmeir et al., 2015; Hewamalage et al., 2022) LGBM benefits from using purged *k*-folds with nested cross-validation (Lainder & Wolfinger, 2022).
       2. Neural Prophet
       3. Recurrent Neural Network (LSTM cells)
  1. Forecast horizon
     1. Compare 1-step and 18-step horizons (18 step was used for monthly data in M3 (Makridakis & Hibon, 2000))

1. Accuracy Measures
   1. MAE for directly comparing model accuracy.
   2. AvgRelMAE (scale independent, robust to outliers, easily interpretable) for comparing accuracy change after data protection: , where , and where denotes protected, denotes original, is the number of adjusted forecasts for series and is the number of series. AvgRelMAE < 1 (> 1) indicates increased (damaged) accuracy on average. Average percentage improvement in MAE of forecasts is (1 – AvgRelMAE) 100. 5% trim on AvgRelMAE is recommended (Davydenko & Fildes, 2013).

**Results and Analysis**

1. Results based on changes to the data.
   1. Accuracy (MAE) for all models broken out by methods/horizons.
      1. Table for each protection method (example for differential privacy)

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Model | Original | |  | |  | |  | |  | |  | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| SES |  |  |  |  |  |  |  |  |  |  |  |  |
| DES |  |  |  |  |  |  |  |  |  |  |  |  |
| TES |  |  |  |  |  |  |  |  |  |  |  |  |
| ARIMA |  |  |  |  |  |  |  |  |  |  |  |  |
| Prophet |  |  |  |  |  |  |  |  |  |  |  |  |
| Greykite |  |  |  |  |  |  |  |  |  |  |  |  |
| LGBM (univariate) |  |  |  |  |  |  |  |  |  |  |  |  |
| VAR |  |  |  |  |  |  |  |  |  |  |  |  |
| LGBM (multivariate) |  |  |  |  |  |  |  |  |  |  |  |  |
| NeuralProphet |  |  |  |  |  |  |  |  |  |  |  |  |
| RNN (LSTM cells) |  |  |  |  |  |  |  |  |  |  |  |  |

* 1. Examine distributions of spectral entropy (forecastability) and coefficient of variation (variability) in instance space before and after each method of data protection.
  2. Calculate change in accuracy for all models/methods/horizons relative to the original data (AvgRelMAE).
  3. Discuss which models had the largest/smallest increases/damages in accuracy.
  4. Examine distributions of time series characteristics (e.g., seasonality, trend) before and after data protection to explain *why* models had increases/damages in accuracy.

1. Results based on adjustment direction.
   1. For each method/model/horizon combination calculate:
      1. Proportion of positive/negative adjusted forecasts.
      2. Change in accuracy (AvgRelMAE) for positive and negative adjusted forecasts.
      3. Bias (mean of forecast errors) for positive and negative adjusted forecasts.
   2. Adapt the following table for our purposes (Fildes et al., 2009).

A screenshot of a computer

Description automatically generated with medium confidence

* 1. Two-sided binomial test for the probability of an adjustment that increases accuracy – use similar table as below (Davydenko & Fildes, 2013).

A picture containing Word

Description automatically generated

1. Results based on size of adjustment.
   1. Compute size of adjustment: (Fildes et al., 2009).
   2. Regressions/ANOVAs
      1. For random noise protection.
         1. Accuracy ~ Size + Noise magnitude + Size Noise magnitude
      2. For top/bottom coding.
         1. Accuracy ~ Size + Degree + Size Degree
2. Model Complexity vs. Accuracy.
   1. Measure complexity using Kolmogorov complexity as described by (Hewamalage et al., 2022)
      1. Train Model 🡪 Save Model (coefficients, objective functions, etc.) 🡪 Gzip Compressed Model 🡪 Approximate Kolmogorov Complexity using size of the compressed model on disk.
   2. Regress Accuracy ~ Complexity.

**Conclusions**

1. General Discussion
   1. Which models performed best on original data.
      1. Why.
   2. Which models performed best on protected data.
      1. Why.
2. Managerial Implications
   1. Limit analysts to simple models when forecasting using protected data.
3. Future Work
   1. Ways to improve forecast accuracy under data protection.
      1. Make adjustments based on methods from judgmental forecasting literature (Fildes et al., 2009)
      2. Like forecasting support systems that actively evaluate and filter information before presenting it (Fildes et al., 2019), design (or implement) methods to filter random noise from the series prior to forecasting.

**References**

Abowd, J. M., Gittings, K., McKinney, K. L., Stephens, B. E., Vilhuber, L., & Woodcock, S. (2012). *Dynamically consistent noise infusion and partially synthetic data as confidentiality protection measures for related time-series*. 41.

Alvarado-Valencia, J., Barrero, L. H., Önkal, D., & Dennerlein, J. T. (2017). Expertise, credibility of system forecasts and integration methods in judgmental demand forecasting. *International Journal of Forecasting*, *33*(1), 298–313. https://doi.org/10.1016/j.ijforecast.2015.12.010

Bergmeir, C., Hyndman, R. J., & Koo, B. (2015). *A Note on the Validity of Cross-Validation for Evaluating Time Series Prediction*. 17.

Boone, T., Ganeshan, R., Jain, A., & Sanders, N. R. (2019). Forecasting sales in the supply chain: Consumer analytics in the big data era. *International Journal of Forecasting*, *35*(1), 170–180. https://doi.org/10.1016/j.ijforecast.2018.09.003

Chen, C., & Liu, L.-M. (1993). Forecasting time series with outliers. *Journal of Forecasting*, *12*(1), 13–35. https://doi.org/10.1002/for.3980120103

Crimi, N., & Eddy, W. (2014). Top-Coding and Public Use Microdata Samples from the U.S. Census Bureau. *Journal of Privacy and Confidentiality*, *6*(2). https://doi.org/10.29012/jpc.v6i2.639

Davydenko, A., & Fildes, R. (2013). Measuring forecasting accuracy: The case of judgmental adjustments to SKU-level demand forecasts. *International Journal of Forecasting*, *29*(3), 510–522. https://doi.org/10.1016/j.ijforecast.2012.09.002

de Montjoye, Y.-A., Radaelli, L., Singh, V. K., & Pentland, A. “Sandy.” (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*, *347*(6221), 536–539. https://doi.org/10.1126/science.1256297

Fildes, R., Goodwin, P., Lawrence, M., & Nikolopoulos, K. (2009). Effective forecasting and judgmental adjustments: An empirical evaluation and strategies for improvement in supply-chain planning. *International Journal of Forecasting*, *25*(1), 3–23. https://doi.org/10.1016/j.ijforecast.2008.11.010

Fildes, R., Goodwin, P., & Önkal, D. (2019). Use and misuse of information in supply chain forecasting of promotion effects. *International Journal of Forecasting*, *35*(1), 144–156. https://doi.org/10.1016/j.ijforecast.2017.12.006

Gonçalves, C., Bessa, R. J., & Pinson, P. (2021). A critical overview of privacy-preserving approaches for collaborative forecasting. *International Journal of Forecasting*, *37*(1), 322–342. https://doi.org/10.1016/j.ijforecast.2020.06.003

Goncalves, C., Bessa, R. J., & Pinson, P. (2021). Privacy-Preserving Distributed Learning for Renewable Energy Forecasting. *IEEE Transactions on Sustainable Energy*, *12*(3), 1777–1787. https://doi.org/10.1109/TSTE.2021.3065117

Goncalves, C., Pinson, P., & Bessa, R. J. (2021). Towards Data Markets in Renewable Energy Forecasting. *IEEE Transactions on Sustainable Energy*, *12*(1), 533–542. https://doi.org/10.1109/TSTE.2020.3009615

Hewamalage, H., Bergmeir, C., & Bandara, K. (2021). Recurrent Neural Networks for Time Series Forecasting: Current status and future directions. *International Journal of Forecasting*, *37*(1), 388–427. https://doi.org/10.1016/j.ijforecast.2020.06.008

Hewamalage, H., Bergmeir, C., & Bandara, K. (2022). Global models for time series forecasting: A Simulation study. *Pattern Recognition*, *124*, 108441. https://doi.org/10.1016/j.patcog.2021.108441

Imtiaz, S., Horchidan, S.-F., Abbas, Z., Arsalan, M., Chaudhry, H. N., & Vlassov, V. (2020). Privacy Preserving Time-Series Forecasting of User Health Data Streams. *2020 IEEE International Conference on Big Data (Big Data)*, 3428–3437. https://doi.org/10.1109/BigData50022.2020.9378186

Kang, Y., Hyndman, R. J., & Smith-Miles, K. (2017). Visualising forecasting algorithm performance using time series instance spaces. *International Journal of Forecasting*, *33*(2), 345–358. https://doi.org/10.1016/j.ijforecast.2016.09.004

Lainder, A. D., & Wolfinger, R. D. (2022). Forecasting with gradient boosted trees: Augmentation, tuning, and cross-validation strategies. *International Journal of Forecasting*, S0169207021002090. https://doi.org/10.1016/j.ijforecast.2021.12.003

Liyue Fan & Li Xiong. (2014). An Adaptive Approach to Real-Time Aggregate Monitoring With Differential Privacy. *IEEE Transactions on Knowledge and Data Engineering*, *26*(9), 2094–2106. https://doi.org/10.1109/TKDE.2013.96

Luo, J., Hong, T., & Fang, S.-C. (2018). Benchmarking robustness of load forecasting models under data integrity attacks. *International Journal of Forecasting*, *34*(1), 89–104. https://doi.org/10.1016/j.ijforecast.2017.08.004

Makridakis, S., & Hibon, M. (2000). The M3-Competition: Results, conclusions and implications. *International Journal of Forecasting*, *16*(4), 451–476. https://doi.org/10.1016/S0169-2070(00)00057-1

Nin, J., & Torra, V. (2009). Towards the evaluation of time series protection methods. *Information Sciences*, *179*(11), 1663–1677. https://doi.org/10.1016/j.ins.2009.01.024

Ozimek, A., DeAntonio, D., & Zandi, M. (2018). Aging and the Productivity Puzzle. *American Economic Association Conference*, 23.

Petropoulos, F., Apiletti, D., Assimakopoulos, V., Babai, M. Z., Barrow, D. K., Taieb, S. B., Bergmeir, C., Bessa, R. J., Bijak, J., Boylan, J. E., Browell, J., Carnevale, C., Castle, J. L., Cirillo, P., Clements, M. P., Cordeiro, C., Oliveira, F. L. C., Baets, S. D., Dokumentov, A., … Ziel, F. (2022). *Forecasting: Theory and practice*. 167.

Reece, A. G., Reagan, A. J., Lix, K. L. M., Dodds, P. S., Danforth, C. M., & Langer, E. J. (2017). Forecasting the onset and course of mental illness with Twitter data. *Scientific Reports*, *7*(1), 13006. https://doi.org/10.1038/s41598-017-12961-9

Schneider, M. J., & Mankad, S. (2021). A Two-Stage Authorship Attribution Method Using Text and Structured Data for De-Anonymizing User-Generated Content. *Customer Needs and Solutions*, *8*(3), 66–83. https://doi.org/10.1007/s40547-021-00116-x

Sommer, B., Pinson, P., Messner, J. W., & Obst, D. (2021). Online distributed learning in wind power forecasting. *International Journal of Forecasting*, *37*(1), 205–223. https://doi.org/10.1016/j.ijforecast.2020.04.004

Sweeney, L. (2002). k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(05), 557–570. https://doi.org/10.1142/S0218488502001648

Véliz, C., & Grunewald, P. (2018). Protecting data privacy is key to a smart energy future. *Nature Energy*, *3*(9), 702–704. https://doi.org/10.1038/s41560-018-0203-3

Wellens, A. P., Udenio, M., & Boute, R. N. (2021). Transfer learning for hierarchical forecasting: Reducing computational efforts of M5 winning methods. *International Journal of Forecasting*, S0169207021001606. https://doi.org/10.1016/j.ijforecast.2021.09.011