Privacy-Preserving Techniques for Machine Learning Applications in Supply Chains

Author: Ayush K. Joshi , Supervisor: Tianyu Li , Responsible Professor: Zekeriya Erkin
Cyber Security Group , Department of Intelligent Systems , Delft University of Technology

Abstract

Supply chains are vital to the global economy, and so, increasing efficiency in supply chain management is of utmost importance. Modernizing technology has allowed for various uses of machine learning to be possible in several aspects of supply chains, specifically in demand forecasting with prediction models, and customer relations with chat-bots. While this may be the case, many organizations are reluctant to implement such solutions due to potential threats to their privacy. In addition to this, some currently existing solutions do not take special care for privacy preservation. This brings the question of, "How can privacy be preserved in machine learning based applications in supply chains?" The results of this survey show that several approaches for privacy-preservation of machine learning applications exist, and can be applied to supply chains while maintaining increased efficiency in supply chain management.

1 Introduction

With the current level of globalization and advancing technology, supply chains have become complex, and integral to any business. With any such systems and new technologies, there are vulnerabilities present, and new issues surfacing. Privacy concerns related to sensitive data and unwanted access have arisen in supply chains, due to the involvement of emerging technologies such as Machine Learning (ML) and Blockchain. In addition to this, concerns about end-user information being acquired by adversaries is also an issue. According to Hassija et al., many organizations have adopted Artifical Intelligence (AI) systems in their businesses, and its use in the future can only be expected to increase due to the offered advantages [11]. Furthermore, applications of ML, a subset of AI, have highly potential applications in supply chains, such as in demand forecasting. While that may be the case, privacy concerns related to sensitive data exist with many ML approaches, and so many stakeholders are reluctant implement such approaches [23].

How can privacy be preserved for ML based applications in supply chains? This paper will address the aforementioned research question, due to its importance, and the growing need for transparency, security, and trustworthiness in associated supply chains [11]. This particular survey will focus on two significant areas for ML applications in supply chains, namely the applications in demand forecasting, and chat-bot usage for customer and supplier relations. For these areas, due to lack of existing implementations of privacy-preserving ML solutions, a survey of existing research will be used to determine the ideal privacy-preserving techniques for future implementations.

2 Background

Supply chains can be complex due to the large volume of involved organizations and various actions. In addition to this, ML is also a diverse field of computer science, and has several applications in supply chains according to industry experts [4]. To explore the possible privacy concerns with such applications, some background information on the relevant topics is required.

2.1 Machine Learning

ML is used to develop applications that learn from experiences and data in order to improve decision-making, or increase prediction accuracy over time [8]. Generally, data sets known as training data are prepared and used to train ML models. Depending on the desired application, the data can be labeled or unlabeled. The training data is then passed through a chosen algorithm to create a model. Several different types of algorithms exist such as Artificial Neural Networks and Support Vector Machines. Other algorithms includes clustering algorithms, association algorithms, and decision trees. After training, the model can then be used with new data for output, as well as for improving the model itself. Because of the nature of these algorithms, the required data, and other related situations, specific privacy concerns can arise [10].

Threats to Privacy in Machine Learning Applications

ML applications can provide significant advantages, such as increases in efficiency of supply chain operations [4]. However, making use of such methods gives rise to privacy threats [16]. Most of these threats are posed to sensitive data due to the nature of supply chains, as the amount of involved parties is high. In addition to this, computations are generally conducted by a party other than the owner of the data, implying a transfer of private data is involved [10]. This poses a high risk to the data, as it becomes susceptible to attacks. The data could then be held for ransom, or be used by third parties

such as competitors. Due to this, many customers are reluctant to implement ML based solutions, despite the significant benefits offered by ML solutions [2]. Some prominent threats to privacy in ML applications are posed by the following attacks:

- Reconstruction Attacks - This threat is related to sensitive data in that Reconstruction Attacks aim to work backwards from features of a data set and reconstruct the private raw data used by the ML model [2]. As a result, even though the features derived from raw data may be unidentifiable, a reconstruction attack can get access to the useful raw data for malicious use.
- Model Inversion Attacks - Such attacks, aim to arrive back at the input data. As ML models do not store raw data or feature data within the model, attackers cannot gain access to the input data, but may still have access to the output. The adversary may instead attempt to create a new model that uses the output, and error data of the ML model to arrive back at the input features [2]. This can then be combined with reconstruction attacks to arrive at raw data.
- Inference Attacks - Membership Inference Attacks attempt to determine whether a sample was part of a specific training data set used to construct the targeted ML model [21]. Such attacks can be used to determine if a sample belongs to a specific class, such as data belonging to one of several companies.
- De-anonymization - De-Anonymization is, as the name suggests, a method to determining the true identity or nature of anonymized data sets. Personal information can be uncovered such as Netflix user data, financial data, and health care records [19]. Although such an example is broad, de-anonymization is applicable to multi-party computations for supply chain applications, especially when computations are conducted by a third party.

Privacy-Preserving Techniques for Machine Learning
While there are several threats to privacy in ML applications, several potential solutions also exist.

- Cryptographic Approaches - One of the best ways to avoid private data falling into the wrong hands is by following cryptographic protocols, especially when multiple input parties are involved [2]. This directly addresses concerns about sensitive data leaks as it tackles the issue of raw data being easily accessible to unwanted parties. In addition to this, such approaches have the added benefits of reducing obstacles to securing multi-party computation, and time-saving benefits.
- Homomorphic Encryption - Although this too is a cryptographic approach, a key differentiating factor from other cryptographic approaches is that the ML computation can be performed directly on the encrypted data, and the output also remains encrypted [12]. This difference offers a significant level of privacy preservation. Homomorphic Encryption offers similar benefits to other cryptographic approaches for sensitive data, in addition, it provides solutions for attacks such as reconstruction attacks, and model inversion attacks, as any result from these would still not be accessible. That being said, fully homomorphic encryption is a costly system [24].
- Garbled Circuits - Garbled Circuits are useful for preserving privacy when the computation involves only two parties. One party generates the garbled circuit, and sends it to the other party, along with its own garbled data. The other party can then evaluate and make use of the garbled circuit with its own garbled input, in order to obtain the results. The use of garbled circuits avoids any leaks of the encrypted data to either parties [13].
- Differential Privacy - Differential Privacy is used to counter inference attacks. This is done by using perturbation approaches through the addition of random noise to the data at different points in the algorithm. The goal of differential privacy is to ensure "...that any sequence of outputs (responses to queries) is "essentially" equally likely to occur, independent of the presence or absence of any individual." [7]. While this is an efficient technique, a certain level of trust is required on the computation party. As a result of this, Local Differential Privacy techniques also exist, which is when the data owners add random noise to the data, eliminating the remaining privacy risks.

2.2 Supply Chains

A supply chain is a network of organizations, stakeholders, operations, information, and resources required to provide any product or service from end to end. Supply chains may involve raw material suppliers, manufacturers, distributors, transporters, customers, and several other possible organizations [16]. Predicting demand for each level in the supply chain is of high importance as balancing supply and demand can greatly improve a supply chain's efficiency [14]. Communication and interaction between the organizations and their customers or suppliers is also equally important. There are ML solutions with great potential for such situations; however, the solutions can be vulnerable.

While the vulnerabilities in supply chains range from counterfeit goods to theft, the vulnerabilities relevant to ML applications and privacy are related with cybersecurity and third party vendor risks [11]. The cybersecurity threats are related to intellectual property, sensitive data, and cloud technology, while third party vendors pose threats to companies' private data. In all cases, the key threats to privacy are related to a company's data being accessed or acquired by unwanted adversaries, with different outcomes depending on the specific threats that were previously mentioned. In order to reduce reluctance of organizations to implement ML solutions in supply chains, the threats must be addressed. Furthermore, in order to avoid the actualization of such threats, currently existing applications of ML in supply chains should also be modified. The scope of this survey concerns two areas in supply chains where ML applications are highly beneficial, which may also be vulnerable. These are demand forecasting, and customer relations through the use of chat-bots.

Demand Forecasting and Forecast Accuracy

Demand forecasting is a process used in supply chains in order to predict future demand of a product based on historical data [15]. Several methods of demand forecasting exist for a variety of different situations, such as seasonal demand of a product or a product with specific trends in its demand. The methods use historical data about demand for the product in order to predict future demand.

Several traditional methods for this already exist, such as:

- Naive Forecast - This simple method uses a previous period's data as a viable prediction for future demand [15].
- Moving Average - This method uses an average of recent historical data to predict future demand [15].
- Trend - Trend based forecasting methods are ideal for predicting future demand of products' demand's that follow specific trends. This too is a relatively simple model, and uses linear regression as its basis [5].
- Multiple Linear Regression - The Multiple Linear Regression method is used to predict changes in future demand by using historical data of changes in demand [5].

While these are effective methods, they can lead to reduced accuracy, and result in the Bullwhip Effect [5]. The Bullwhip Effect refers to an occurrence in distribution channels when distortions in each stage of of a supply chain cause the change in accuracy of the next stage to be larger [15]. Slight inaccuracies in the demand forecasting of retailers can compound onto manufacturers, and so on through to suppliers. This causes large inefficiencies in the operations of a supply chain.

In order to reduce the forecasting errors, over the past decade or so, several algorithmic approaches which make use of ML algorithms have been implemented. Some prominent approaches are with Artificial Neural Networks (ANN), Recurrent Neural Networks (RNN), and Support Vector Machines (SVM). ANNs are based on the neural networks of a human brain, consisting of layers of neurons (nodes) to which input is given and the desired data is acquired as output. Carbonneau states that Feed-Forward Error Back-Propagation Type neural networks are most commonly used in demand forecasting [14]. Feed-Forward refers to the acyclical nature of the connections between nodes, meaning the output of one layer is passed on as input to the nodes of the next layer only, moving in one direction. Back-propagation of error is a method of training ANNs in which a loss function is used to determine the error, and is propagated back through the layers in order to increase accuracy. This increases the efficiency in demand forecasting [5].

While ANNs consist of feed-forward networks, RNNs allow for the output of neurons to travel backwards as input for the same or previous layers. RNNs are especially applicable for time-series demand forecasting, as an alternative to traditional methods such as Holt's Method. While ANNs and RNNs aim to minimize the forecasting error, SVMs aim to minimize the margin of error [5].

While these methods have been effective, historically few precautions have been taken in order to preserve privacy when applying such techniques in supply chains. Because of this, it is important to identify which threats to privacy exist in ML applications, and what the potential solutions are.

Chat-bot Usage in Supply Chains

A chat-bot is simply a piece of software that is used to imitate human communication capabilities to provide a desired response to a query entered by any given user. Old generation chat-bots lacked flexibility, being able to only respond correctly to a fixed set of inputs. In order to design a good chat-bot, it is important to understand which characteristics it should display. In essence, a good chat-bot should understand natural language input, manage dialogue, respond with natural language, and preserve the privacy of both the user and the developer [22]. According to Dr. Nuruzzaman there are essentially four classifications of chat-bots; goal-based, knowledge-based, service-based and response generated-based. Goal-based chat-bots designed for a specific task and only for short conversations, getting inputs from the user in order to complete said task. Knowledge-based chat-bots are classified based on what type of data source they are gathering their data from, either closed domain or open domain. Service-based chat-bots are aptly named because they essentially provide a service to the user like ordering a meal or making an appointment without the intervention of a human. Lastly, response generated-based chat-bots are defined by what kind of action they execute when responding to the user [18].

The earlier methods used to develop chat-bots did not use ML approaches, instead they mainly used pattern matching and rule-based methods.

- Pattern matching: chat-bots based on pattern matching theory were used in situations where the scenario was one of the users asking questions and the chat-bot answering them [22]. The software would be developed such that it would match the input of the user to a set of predefined questions and return a template answer based on that match. A.L.I.C.E. is a chat-bot developed by Richard Wallace is a good example of a chat-bot based on pattern matching algorithms [22].
- Rule-based: chat-bots developed with the rule-based approach work on the principle of mapping the user's input and associating it with the database. The software reads the input by turning it into a so-called keystack and marking some predefined keywords with the highest frequency. It then uses the frequency of the keywords to associate the input with a category of response, resulting in a more adaptable response as compared to a pattern matching chat-bot [22]. Some examples of chat-bots that utilize a rule-based approach are ELIZA by Weizenbaum and PARRY by Colby, both in the latter half of the 20th century.

Considering this, it can be seen how the above approaches for developing chat-bots caused them to be less flexible. Chat-bots have several applications in supply chain management, such as tracking and order related issues, providing information to customers and conducting surveys. ML can be used to greatly enhance the performance of chat-bots, such that they could perform at the level of human operators.

3 Survey Contribution

The Case for Privacy-Preserving ML in Supply Chains

While there are some existing privacy-preserving ML applications, the scope of the applications is higher still. Many of the existing uses of ML for supply chains do not take privacy preservation into account, or organizations are still reluctant to implement ML solutions do to the privacy concerns [23]. As such, it is beneficial for current ML solutions to have privacy-preserving techniques implemented, and more importantly, the awareness of the privacy-preserving techniques for reluctant organizations also needs to be raised. Due to the lack of available resources that discuss supply chains, privacy-preservation, and ML, it is difficult for the two points mentioned above to be addressed. The goal of this survey is to do just so. As such, section four will discuss the different privacy-preserving techniques that exist for ML, as well as their advantages, disadvantages, and applicability to areas in supply chains. Specifically for demand forecasting, and chat-bot usage in customer relations.

Section four will also contain information on the motivation of using ML approaches for demand forecasting and customer relations. In addition to this, there is also a discussion of an example of existing privacy-preserving ML in demand forecasting, and the current usage of chat-bots in customer relations. Finally, there is also a discussion of which of the techniques would be applicable for different application areas.

4 Research and Results

4.1 Machine Learning in Demand Forecasting

Research shows that ML approaches for demand forecasting increased accuracy when compared to traditional methods [5]. In addition, more approaches using artificial neural networks showed promising results in a study conducted by Kochak et al.[14]. ML approaches such as Artificial Neural Networks (ANN), Recurrent Neural Networks (RNN), and Support Vector Machines (SVM) can be used for demand forecasting. A study conducted by Carbonneau et al. discovered that these techniques are, in fact, more accurate and reduce the forecasting error, as can be seen on the right in the extract of results from the study.

Forecasting technique	Testing set	
	MAE	Std. dev.
RNN	447.72	328.23
LS-SVM	453.04	341.88
MLR	453.22	343.65
NN	455.41	354.40
Naïve	520.53	407.29
Moving average	526.61	370.35
Trend	618.02	487.42

Figure 1: Comparison of the Performance (MAE) of Forecasting Techniques

As evidenced, RNNs and SVMs provide a lower Mean Average Error (MAE) and lower standard deviation. While the traditional method of multiple linear regression performs slightly better than ANNs, it was explained in the study that this was caused due to over fitting on the training data. Furthermore, it was concluded that such techniques increase forecasting accuracy, decrease costs, and increase customer satisfaction [5]. The paper also noted that using the techniques as designed in the study is only viable for single party operations, since there factors that are hurdles for collaboration [5]. While these ML techniques may be used by organizations to predict demand without outside information, it is ideal to have collaboration with other parties involved in the supply chain, such as suppliers and customers [16]. This would allow for more valuable data to be available for demand forecasting, thus allowing for higher accuracy, and allow increased efficiency in supply chain management in the long term. While the advantages of ML solutions are significant, the ML techniques used can be susceptible to model inversion attacks, inference attacks, and reconstruction attacks. This means that techniques for privacy preservation would be useful in order to promote the collaboration.

4.2 Chat-bot Usage in Supply Chains

With the advent of technologies like machine and deep learning, computer scientists were able to take the large amounts of data gathered through supplier/customer interactions and train a chat-bot to be more versatile. Thus, the chat-bot would be able to give correct responses to a much wider range of queries, and at the same time respond to those queries with more realistic and human-like communication patterns. A crucial part of supply chain management is the interaction between supplier and customer, one that requires human capital to establish and maintain. With the increasing capabilities of personal assistants like Siri, Alexa, and Google Assistant, it is not difficult to imagine how similar intelligent chat-bots can make a significant impact on this aspect of supply chain management.

A study conducted by Lei Cui et al. on the customer service SuperAgent, covers important customer-company based relations such as FAQs and chit-chat conversation on E-Commerce websites. Cui provides an example of ATT using this chat-bot to answer people's FAQs in a chat, including natural language like chit-chat [6]. ML is already making an impact in supply chains due to its practical applications and offered advantages. Some of the use cases are discussed in a conference paper by Hannah Wenzel et al., where the three areas of focus are Selecting Supply Chain Partners, Demand Forecasting for DM (one of Germany's largest drugstore companies) and Detecting False-Positive RFID Tag Reads [25]. All three of these applications can be argued to be more complex in nature than what is expected of a ML based chat-bot, especially the selection of supply chain partners and demand forecasting. From this, it is evident that not only will implementing ML based chat-bots free up human capital in supply chain processes, but it also allows for around the clock availability and support for any customer queries in order to reduce inefficiencies in supply chain management.

In this age of increasingly intermingled technology in human lives, privacy preservation is of high importance. Although it appears simple when an organization states that user data will be fed to ML algorithms in order to improve chat-

bots, it is important to concretely define from where and how the data will be collected, as well as which data will be collected. As with all developing technologies, chat-bots also have their disadvantages. For the purposes of this survey, the main focus will be on the privacy vulnerabilities of chat-bots. The foremost privacy issue in ML based chat-bots is the large amounts of data that is required in order develop a model and have a well functioning chat-bot. There are many debates as to where the data will be collected from, and many raise concerns about the in-home, always-on devices such as Alexa and Google Home [20]. Considering this, there are several ethical concerns about how the data will be collected. These privacy concerns only pile onto an audience which is already skeptical of the use of technologies like ML and AI in everyday life, from an ethical standpoint.

One of the biggest advantages that ML presents to the field of chat-bots is allowing them to communicate in a more human-like manner. Because of this, there are several areas where ML can be implemented. As briefly mentioned earlier, these areas include Natural Language Processing (NLP), Natural Language Understanding (NLU), Dialogue Management (DM), and Natural language Generation (NLG) [22]. ML can be used to identify the emotions of the user interacting with the chat-bot, and thus return a proper response to the user according to their mood. For this, DM is used to decide the category of the database from which the chat-bot will pull its response. The next stage is generating a response that seems like a human wrote it, for which NLG is used. It also allows for personalized and immediate natural language responses made by chat-bots [22].

The reason why so much research is being conducted into ML based chat-bots is because of the offered increase in optimization of supply chain processes, along with the introduction of cost saving measures for corporations. chat-bots are aimed to replace human agents, for which corporations currently have high expenditure. In a study mentioned in Martin Adam's paper on AI-based chat-bots in customer service, it is mentioned that as of 2019, chat-bots could effectively reduce global business expenditures of roughly $1.3 trillion by 30% related to customer service inquiries [1]. This significant impact would be created by using chat-bots to decrease the response times, freeing human capital and dealing with up to 80% of frequently asked questions. The paper goes on to state that chat-bots can save up to $8 billion per year by the year of 2022. From this, it is evident that not only will implementing ML based chat-bots free up human capital in supply chain processes, but it also allows for around the clock availability and support for any customer queries. While that is the case, the privacy concerns regarding data of users with chat-bots are high. This is mostly related with re-identification of user data [19]. A prominent example of this was a study conducted at the University of Texas, where personal data and identities of Netflix users were easily uncovered. Similarly, other personal data such as financial and health care records can be at risk [19].

4.3 Privacy Preserving Techniques for Machine Learning Applications in Supply Chains

Cryptographic Approaches - An Example

Cryptographic approaches for privacy-preservation are common due to the best practices considered when transferring sensitive data between parties. Some cryptographic privacy-preserving ML techniques already exist for demand forecasting. A paper by Fabian Taigel et al. discusses the reluctance of customers to provide condition data to suppliers for demand forecasting usage due to privacy concerns [23]. Due to this a privacy preserving method of supervised ML was used, with order preserving encryption. The paper states that without privacy preserving techniques, normally one maintenance, repair, and overhaul service provider (MRO) serves multiple customers. This is done by customers individually determining when a part needs MRO, and the order is sent to the provider. This is inefficient as MRO providers cannot predict when specific parts will be required especially for air crafts, and as previously stated, customers are reluctant to share the private data.

The alternative to this is the concept of the ML approach suggested in the paper. This entails the use of real-time condition data from multiple customers for all parts. The data is secure on the customers' encrypted databases, and they hold the key. The process takes six distinct steps [23].

1. MRO provide discovers a probabilistic decision tree model on a training data set.
2. Next, the decision tree is translated into basic SQL queries.
3. The queries are then encrypted in order to be executable on encrypted databases that contain the sensitive data of several customers.
4. In step 4, part of the classification function is applied on the encrypted data.
5. The results are then aggregated using a privacy-preserving aggregation protocol, also described in detail in the paper.
6. Finally, the results are obtained, which indicate the predicted demand, and demand forecast's accuracy.

The paper concludes that an approach such as the one described above allows for increased efficiency in demand forecasting and forecasting accuracy, due to the possible collaboration of customers after the threats to sensitive data was addressed. Other substantial benefits include a reduction in service times, and lower inventory costs for the MRO provider. Furthermore, this approach does not neglect the forecast accuracy, which is an equally important aspect of demand forecasting [23].

Such approaches display the feasibility and high potential privacy-preserving ML approaches have in supply chains. As a result, privacy concerns held by other parties in a supply chain can be addressed, while still increasing the performance of demand forecasting in terms of accuracy, and reduced costs of operations, both in time and a financial sense.

Homomorphic Encryption Approaches

Homomorphic Encryption differs from other encryption approaches in the sense that the computation can be performed directly on encrypted data. Due to this key difference, it allows for increased privacy-preservation and defense against certain attacks. An encryption is considered to be homomorphic if, "from Enc(a) and Enc(b) it is possible to compute Enc(f(a, b)), where f can be +, x, $\oplus$, and without using the private key," [24]. As can be seen in this definition and the details of the paper by Taigel et al., the approach mentioned above requires the private key. In addition to this, the operations for that privacy-preserving approach were not limited to +, x, and $\oplus$ operations, which was due to high cost.

With cost in mind, homomorphic encryption can be further differentiated into fully homomorphic encryption, additive homomorphic encryption, and multiplicative homomorphic encryption. Considering the relatively high costs of frequently bootstrapping cipher texts, fully homomorphic encryption approaches are generally not preferred [2]. Instead, additive homomorphic encryption is preferred for privacy preserving ML approaches. Such a system conducts addition operations on the encrypted data, while multiplication operations are done with plaintext. A well known example of this is the Paillier Cryptosystem.

Such techniques are used in order to avoid high costs, with the loss of efficiency and functionality. In order to make up for this, protocols to perform secure multiplication and decryption operations were developed. In addition to this, data packing techniques that enable multiple plain text values to be encrypted by the same cipher text were also developed. In order to develop a system that is efficient and privacy-preserving, a combination of the aforementioned techniques with additive homomorphic encryption were proposed for the collaborative filtering system by Erkin et al. [9].

There are several advantages and disadvantages of Homomorphic Encryption approaches. While fully homomorphic encryption approaches can be highly secure, they have high costs. On the contrary, additive homomorphic approaches have reduced functionality, and if no special measures are taken for increasing functionality, in terms of privacy, the threats to privacy still remain. A system like that would be vulnerable not only to insider attacks on the sensitive data, but specific ML algorithms would also be open to model inversion attacks, inference attacks, and reconstruction attacks. This results from the fact that some of the data would have to be decrypted. That being said, the disadvantages of additive homomorphic encryption approaches can be mitigated with the use of the techniques mentioned above, resulting in a privacy-preserving system and maintaining the functionality. The only drawback such a system has is the vulnerability to insider attacks, which can be possible if involved parties collude. While such a possibility is low due to the separation of organizations in supply chains (e.g. different companies), the possibility still exists, because of which other techniques should also be explored.

Garbled Circuits

The use of garbled circuits is also a potential privacy-preserving approach. Garbled circuits are for computations involving two parties. Because of this, such a privacy-preserving technique is applicable to demand forecasting uses as computations are generally conducted by another organization. In addition to this, private data about sales from retailers can be kept secure from suppliers. The figure below describes a garbling scheme, which provides a simplified overview of how a garbled circuit works in practice.

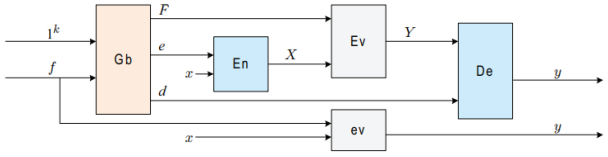

Figure 2: Components of a garbling scheme G = (**Gb, En, De, Ev, ev**). Function **Gb** maps f and k to (F, e, d), strings encoding the garbled function, the encoding function, and the decoding function. Possession of e and x lets one compute the garbled input $\boldsymbol{X}$ = **En**(e, x); having F and X lets one calculate the garbled output Y = **Ev**(F, X) and knowing d and Y lets one recover the final output y = **De**(d, Y), which must equal **ev**(f, x).

[3]

The generator of the garbled circuit would not have access to the evaluator's data. In addition to this, the evaluator only gains the garbled input of the generator, keeping the secure as well. Moreover, research conducted by Huang et al. discuss the efficiency and significantly fast run times of a garbled circuit approach [13]. The framework suggested not only offers improvements in run times by a whole order of magnitude, but also mention how the garbled circuit approach can be more beneficial to other custom protocols or homomorphic approaches. Huang et al. also conclude that simple pipelined garbled circuits are quite applicable and scalable to a vast variety of situations, with modifications to minimize the circuit size [13]. This is especially beneficial in demand forecasting, as input data can range all the way from real-time sensor data to historical sales data.

Differential Privacy and Perturbation Approaches

Perturbation approaches consist of introducing random noise in different steps of the system. This can be done to the input data, intermediate data through the algorithm, or output data. Such techniques are used in conjunction with Differential Privacy. As stated earlier, the goal of differential privacy is to ensure "...that any sequence of outputs (responses to queries) is "essentially" equally likely to occur, independent of the presence or absence of any individual." [7]. Meaning, if any individual data point is included in a data set that is being computed on, the inclusion or exclusion of it will be unknown. As a result, differential privacy is especially useful to counter inference attacks, and de-anonymization. In addition to this dimensionality reduction approaches such as Principal Component Analysis (PCA), a specific type of perturbation approach, allow for security against reconstruction attacks [2].

Differential Privacy algorithms are randomized. The approach of the randomization can be categorized into different types, which were mentioned earlier.

- Input Perturbation - With this method, the random noise is added to the input data. The computation is then done on the randomized input, and the output is thus differentially private. Dwork et al. discuss an example of this with a PCA algorithm. The group added a symmetric Gaussian noise matrix to the co-variance matrix and then followed the steps of the algorithm [7]. Such a method is useful when the value of the sensitive data lies in the input data.
- Output Perturbation - This method regularly conducts computations on the input data, without special conditions ensuring privacy. Once this is done, the random noise is then added to the generated model [2]. While such a method would not provide enough security against attacks on the input data or model reconstruction attacks, it does safeguard the output data. As a result, if the input data is kept secure with other means, and the value lies with the output, output perturbation would be an appropriate method for Differential Privacy.
- Algorithm Perturbation - This method adds random noise to the intermediate values in an algorithm, iterative algorithms to be exact. Due to this, ML algorithms such as PCA and Deep Learning algorithms can be differentially private. In addition, Algorithm Perturbation counters model inversion attacks, and reconstruction attacks, as any generated models from such attacks would be obsolete due to the randomization of the intermediate values.

While these perturbation methods can be effective for differential privacy, the privacy-preservation depends on the fact that the data which is computed on can only be from a single trusted server [2]. Because of this, when multiple parties are involved, such as the MRO example by Taigel et al. mentioned above, these perturbation approaches would not be good alternatives [23].

4.4 Discussion

As can be seen from the techniques mentioned above, the techniques have varying advantages and disadvantages. Due to this, different privacy-preserving techniques are better suited for different situations, depending on the type of ML approach that is already being used, the specifics of the data that is to be used, or the requirements of a specific organization or industry. Considering the varying advantages and disadvantages, the topic merits discussion. The table on the right briefly states the associated advantages, disadvantages, and general use cases for each of the privacy-preserving techniques, in the context of ML and supply chains.

Table 1: Advantages, Disadvantages Potential Application Areas for Privacy-Preserving Techniques

Privacy - Preserving Techniques	Advantages	Disadvantages	Potential Application
General Cryptographic Approaches	• Fits to specific situation • Safeguards against data leaks • Allows multiple parties to collaborate	• Not generalizable • Susceptible to model inversion attacks • Susceptible to reconstruction attacks	• MRO example • Situations with sensitive input or output data • Situations where runtime and costs are unimportant factors
Homomorphic Encryption Approaches	• Safeguards against data leaks • Safeguards against reconstruction attacks • Safeguards against de-anonymization • Safeguards against inference attacks • Allows multiple parties to collaborate	• Fully homomorphic encryption is costly • Additive homomorphic encryption loses functionality, required other techniques to be viable	• Situations with sensitive input and output data • Situations where insider attacks are possible, or white-box knowledge is known to adversaries • Situations where runtime and costs are unimportant factors
Garbled Circuits Approaches	• Safeguards against data leaks • Safeguards against reconstruction attacks • Safeguards against de-anonymization • Safeguards against inference attacks • Offers significantly fast run times compared to older methods and other approaches • Not susceptible to insider attacks • Applicable to wide variety of use cases	• More than two parties cannot use this approach • Standard garbled circuit approaches can be low and inefficient compared to other methods • May remain susceptible to insider attacks if collusion between members of the two parties occurs	• Useful for collaboration in situations with two parties, e.g suppliers and retailers • Applicable to situations where data owners outsource computation • Applicable to cases where faster run times are required
Differential Privacy Approaches	• Safeguards against data leaks • Safeguards against reconstruction attacks • Safeguards against model inversion attacks • Safeguards against de-anonymization • Safeguards against inference attacks • Allows multiple parties to collaborate	• Does not allow computation on data from multiple server sources • Perturbation can cause lossy encryption, causing inefficient processing	• Applicable to use cases where re-identification is a large threat, such as with user records, personal individual information • Applicable in areas where accuracy is not of high importance

Cryptographic Approaches

Cryptographic approaches, excluding Homomorphic Encryption approaches, are primarily advantageous against sensitive data being acquired or accessed by adversaries. In addition to this, because of the nature of such an approach, a custom-tailored system can be implemented to best fit the situation. As was seen in the example discussed earlier, Taigel et al. created a cryptographic approach for forecasting the demand of aircraft MRO parts (Maintenance, Repair, Overhaul), with real-time data about the condition of the parts [23]. Due to this approach, the collaboration of multiple parties was possible, as the concern of data leakage was addressed.

While the advantages are apparent, disadvantages also exist. For example, this kind of approach has high costs in terms of time and manpower, as designing and implementing a solution to a specific situation requires more research, planning, and time for implementation, such as the case with the MRO example. This is because other than standard encryption of data during transferring, specific methods have to be developed for each situation, and so it is not generalizable. In addition to this, while the input and output data may be encrypted, often times it has to be decrypted for computation, which makes some cryptographic approaches susceptible to model inversion attacks, and reconstruction attacks.

Nonetheless, such an approach is still applicable to a wide number of situations. For example, when the privacy concerns are only related to the input or output data, a cryptographic approach can be a good fit. Especially when data about sales, revenue, or performance is being used in demand forecasting. Furthermore, it can also be used for data related with chat-bot usage as user records and personal data can be kept secure.

Homomorphic Encryption Approaches

This specific cryptographic approach offers several advantages, and addresses the shortcomings mentioned in the subsection mentioned above. In addition to safeguarding against data leaks, fully homomorphic encryption approaches can also defend against de-anonymization, inference attacks, and reconstruction attacks. This is a significant addition as the sensitive data can be kept secured, despite having multiple parties involved.

That being said, disadvantages such as high costs due to refreshing ciphertexts. In addition to this, in order to avoid the higher costs aditive homomorphic encryption is used, but at the expense of functionality when compared to fully homomorphic encryption approaches.

Despite the disadvantages, fully or partially homomorphic encryption approaches can still be of great use in situations with sensitive input or output data, systems susceptible to insider attacks, and situations where run times and costs are not of significance. For example, this would not be a good approach for demand forecasting of fast-fashion products due to the short selling times [17]. However, it may be a good approach for chat-bot training and development as homomorphic approaches safeguard against re-identification and inference attacks.

Garbled Circuits Approaches

Garbled circuits are useful for preserving privacy by addressing threats such as data leaks, reconstruction attacks, de-anonymization, inference attacks. In addition to this, modern approaches offer significantly faster run times even when compared to homomorphic approaches. Furthermore, there is a wide range of applicability.

While the advantages are numerous, there are some disadvantages as well. The most prominent one is that garbled circuits are a good approach when only two parties are involved. For example, a retailer and its supplier. It cannot allow for multiple parties. Furthermore, garbled circuits are still susceptible to insider attacks on the input data if collusion occurs between members of the two parties.

Although there are some disadvantages, garbled circuits can be an excellent technique for ML based applications in supply chains. This is especially true for collaboration between two closely working organizations, such as retailers and suppliers in the clothing industry. In addition to this, the fast run times also have potential for future implementations where real-time data is used. This has high potential for demand forecasting in the fast fashion industry, more of which will be discussed later.

Differential Privacy Approaches

Differential privacy approaches have the advantages of safeguarding against data leaks because of the perturbation. In addition to this, such approaches are also useful to defend against reconstruction attacks, and model inversion attacks. Furthermore, the very basis of differential privacy doesn't allow inference attacks and re-identification.

While the advantages are numerous, the disadvantages could cause hurdles. For example, additional data transfer is required if multiple data sources or multiple parties are involved. In addition to this, the random noise added can cause lossy transformations, which reduces accuracy.

While differential privacy approaches can be used for some cases of demand forecasting, the accuracy is of utmost importance and so it may not be the best solution. That being said, it is an excellent technique to preserve privacy in the development and training of chat-bots, since inference attacks and re-identification are prominent threats for the related data.

5 Responsible Research

As this paper is a survey, the research was primarily based on existing work by other authors. Furthermore, no experiments were conducted during the research process. The existing works such as papers, journal articles, and other publications was discovered through different tools such as Google Scholar, WorldCat and the IEEExplore Digital Library. After discovery of the resources, the information was collected and inferences were made in an unbiased manner.

The research was kept unbiased by making use of resources that show several aspects of the topics, not only positive or negative aspects. For example, the study conducted by Carbonneau et al. also included the negative performances of ML solutions [5]. In addition, advantages and disadvantages of the techniques were discussed in order to have a balanced and unbiased overview.

Because of the availability of the tools used, and the approach to the research, such a method is highly reproducible by others. This is because the conclusions drawn from the research were based on the resources used, and so it is likely that others following a similar method would arrive at similar conclusions; which is that the different privacy-preserving techniques are applicable in a variety of areas depending on the requirements of the situation. In addition, because of this unbiased approach, the research was conducted ethically and responsibly.

6 Conclusions and Future Work

The goal of this survey was to determine how privacy can be preserved for ML based applications in supply chains, specifically in the area of demand forecasting, and customer relations through chat-bots. ML applications are advantageous because of the benefits they offer, such as increased accuracy and efficiency in demand forecasting, and the increased quality of chat-bots. Due to the applications the efficiency of supply chain management can be increased. In order to address privacy concerns of organizations not yet using ML solutions in supply chain management, and also non-privacy-preserving solutions, this survey will be useful.

It can be concluded that in most cases issues concerning privacy were related to the data being used in the ML algorithms, whether it was as a direct threat to the data, or through other approaches such as attacks on the ML model. Threats such as data leaks, Model Inversion Attacks, Reconstruction Attacks, Inference Attacks, and De-Anonymization were identified as prominent threats for supply chain use cases of ML. In addition, it was seen that many of these threats lead to an adversary getting access or acquiring sensitive data or feature vectors. In order to address the possible threats, some privacy-preserving techniques were also identified, such as general Cryptographic Approaches, Homomorphic Encryption Approaches, Garbled Circuit Approaches, and Differential Privacy Approaches. It was discussed that the different advantages and disadvantage of each of the approaches, as well as the specifics of the situation and ML algorithm used, allow for the techniques to be applied to a wide variety of situations for demand forecasting and customer relations in order to preserve privacy. In addition to this, because of the nature of the techniques, it is also possible for them to be used with other ML applications in supply chains, such as more accurate delivery prediction.

It can be concluded that general cryptographic approaches are beneficial preserving the privacy of sensitive data, and for collaboration of multiple parties. Homomorphic encryption approaches would be most suited to safeguard against data leaks, inference attacks, de-anonymization, and reconstruction attacks, while also allowing multiple parties to collaborate. Garbled circuits offered fast run times and all the benefits mentioned previously, while only allowing two parties to be involved. These three approaches are ideal for ML applications in demand forecasting. In addition to this, the technique with differential privacy approaches may also be used for demand forecasting applications, but is not ideal due the potential for reduced accuracy of the model because of the random noise added to the data. Instead, it is an ideal approach for ML applications in chat-bots for customer relations, as it safeguards against several attacks, and re-identification, meaning user records or personal data would be secure, and identification of an individual would not be possible.

Considering the reasons mentioned above, it can be concluded privacy can be preserved through several different techniques for a wide variety of situations involving ML applications in supply chains, especially for demand forecasting and customer relations. That being said, the topic is ripe for future work. One prominent example is demand forecasting in the fast fashion industry, for companies such as HM and Zara. As of now, demand forecasting in the fast fashion industry is not common due to long replenishment lead times, short selling seasons, and unpredictable demand [17]. This leads to inaccurate forecasts. ML approaches for demand forecasting in the fast fashion is an excellent solution. Some research has been conducted into the usefulness of ANNs for this. Companies in this industry are large and so value the privacy, of themselves as well as end-users, quite highly. An interesting field of research for future work would be to determine which privacy-preserving techniques would fit the requirements of a novel ML solution for demand forecasting in the fast fashion industry.

References

[1] Martin Adam, Michael Wessel, and Alexander Benlian. Ai-based chatbots in customer service and their effects on user compliance. *Electronic Markets*, Mar 2020.

[2] Mohammad Al-Rubaie and J. Morris Chang. Privacy preserving machine learning: Threats and solutions. *CoRR*, abs/1804.11238, 2018.

[3] Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. Foundations of garbled circuits. In Ting Yu, George Danezis, and Virgil D. Gligor, editors, *the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 16-18, 2012*, pages 784–796. ACM, 2012.

[4] Kostiantyn Bokhan. Machine learning in supply chain: 8 use cases that will impress you, Nov 2020.

[5] Réal Carbonneau, Kevin Laframboise, and Rustam M. Vahidov. Application of machine learning techniques for supply chain demand forecasting. *Eur. J. Oper. Res.*, 184(3):1140–1154, 2008.

[6] Lei Cui, Shaohan Huang, Furu Wei, Chuanqi Tan, Chaoqun Duan, and Ming Zhou. SuperAgent: A customer service chatbot for E-commerce websites. In *Proceedings of ACL 2017, System Demonstrations*, pages 97–102, Vancouver, Canada, July 2017. Association for Computational Linguistics.

[7] Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.*, 9(3-4):211–407, 2014.

[8] IBM Cloud Education. What is machine learning?, Jul 2020.

[9] Zekeriya Erkin, Thijs Veugen, Tomas Toft, and Reginald L. Lagendijk. Generating private recommendations efficiently using homomorphic encryption and data packing. *IEEE Trans. Inf. Forensics Secur.*, 7(3):1053–1066, 2012.

[10] Tianyu Gu, Kang Liu, Brendan Dolan-Gavitt, and Siddharth Garg. Badnets: Evaluating backdooring attacks on deep neural networks. *IEEE Access*, 7:47230–47244, 2019.

[11] Vikas Hassija, Vinay Chamola, Vatsal Gupta, Sarthak Jain, and Nadra Guizani. *IEEE Internet Things J.*, 8(8):6222–6246, 2021.

[12] homomorphicencryption.org. Homomorphic encryption standardization: Introduction.

[13] Yan Huang, David Evans, Jonathan Katz, and Lior Malka. Faster secure two-party computation using garbled circuits. In *20th USENIX Security Symposium, San Francisco, CA, USA, August 8-12, 2011, Proceedings*. USENIX Association, 2011.

[14] Ashvin Kochak and Suman K Sharma. Demand forecasting using neural network for supply chain management. 2014.

[15] Xishu Li. Lecture: Demand forecasting - technology operations and management course, Nov 2020.

[16] Sandhya Makkar, Dr G.Naga Rama Devi, and Vijender Solanki. *Applications of Machine Learning Techniques in Supply Chain Optimization*, pages 861–869. 01 2020.

[17] Maria Elena Nenni, Luca Giustiniano, and Luca Pirolo. Demand forecasting in the fashion industry: A review. *International Journal of Engineering Business Management*, 5:37, 2013.

[18] Mohammad Nuruzzaman and Omar Khadeer Hussain. A survey on chatbot implementation in customer service industry through deep neural networks. *2018 IEEE 15th International Conference on e-Business Engineering (ICEBE)*, 2018.

[19] C. C. Porter. [5shidlerjlcomtech003] de-identified data and third party data mining: The risk of re-identification of personal information. 2008.

[20] Elayne Ruane, Abeba Birhane, and Anthony Ventresque. Conversational AI: social and ethical considerations. In Edward Curry, Mark T. Keane, Adegboyega Ojo, and Dhaval Salwala, editors, *Proceedings for the 27th AIAI Irish Conference on Artificial Intelligence and Cognitive Science, Galway, Ireland, December 5-6, 2019*, volume 2563 of *CEUR Workshop Proceedings*, pages 104–115. CEUR-WS.org, 2019.

[21] Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. Membership inference attacks against machine learning models. In *2017 IEEE Symposium on Security and Privacy, SP 2017, San Jose, CA, USA, May 22-26, 2017*, pages 3–18. IEEE Computer Society, 2017.

[22] Prissadang Suta, Pornchai Mongkolnam, Jonathan Chan, Xi Lan, and Biting Wu. An overview of machine learning in chatbots. *International Journal of Mechanical Engineering and Robotics Research*, 9:502–510, 04 2020.

[23] Fabian Taigel, Anselme K. Tueno, and Richard Pibernik. Privacy-preserving condition-based forecasting using machine learning. *Journal of Business Economics*, 88(5):563–592, Jul 2018.

[24] Maha Tebaa and Said El Hajji. Secure cloud computing through homomorphic encryption. *CoRR*, abs/1409.0829, 2014.

[25] Hannah Wenzel, Daniel Smit, and Saskia Sardesai. A literature review on machine learning in supply chain management. In Wolfgang Kersten, Thorsten Blecker, and Christian M. Ringle, editors, *Artificial Intelligence and Digital Transformation in Supply Chain Management: Innovative Approaches for Supply Chains. Proceedings of the Hamburg Int*, volume 27 of *Chapters from the Proceedings of the Hamburg International Conference of Logistics (HICL)*, pages 413–441. Hamburg University of Technology (TUHH), Institute of Business Logistics and General Management, 2019.