Towards Trusted Data Processing for Information and Intelligence Systems

Yong Wang
Dakota State University
Yong.Wang@dsu.edu

Kaushik Ragothaman
Dakota State University
Kaushik.MuthusamyRagothaman
@trojans.dsu.edu

Bijay Shakya
Dakota State University
Bijay.Shakya@trojans.dsu.edu

Abstract

Data is a valued asset and its security is essential for any enterprise and organization. This paper introduces Trusted Data Processing (TDP) and addresses three fundamental questions in TDP: 1) what are the essential requirements to achieve TDP? 2) what security mechanisms and safeguards are available to ensure TDP? 3) how to integrate TDP to practice? Based on the attacks targeting at data assets and their consequences, the requirements to achieve TDP, including data security, data privacy, accountability, transparency, distributed computing, and trusted elements, are identified. Available security mechanisms and safeguards to ensure TDP are discussed. This paper also summarizes the challenges to achieve TDP and provides a practical guidance to achieve TDP through the integration with NIST Cybersecurity Framework.

1. Introduction

Every industry today aims to be data-driven [1]. Decisions are made based on actual data rather than intuition or observation alone. To support data-driven decision making processes, large amount of data has been created and made available. According to IDC, the ‘Global Datasphere’ in 2018 reached 33 zettabytes and will grow to 175 zettabytes in 2025 [2]. Data has become an important asset for enterprises and organizations. It can generate value not only for present but also for future [3]. Due to the importance of data to the decision-making processes, data security is essential for any business operation in any organization. According to a recent survey by Netwrix, 74% organizations in the survey named data security as the top IT priority in 2020 [4]. Many efforts have been conducted in enterprises and organizations to improve cybersecurity. Cybersecurity spending has been on the rise for the past several years. It increased by 141% from 2010 to 2018 [5]. In 2019, spending on information security products and services was estimated at $124 billion [5].

Many safeguards have been placed in enterprises and organizations to ensure data security. Defense-in-Depth (DiD) approach is often used when securing data assets. In a Defense-in-Depth approach, data assets are usually surrounded by layers of safeguards including security and privacy controls in software, computers, communication networks, and perimeter [6]. Despite the fact that cybersecurity spending continues to grow and many more safeguards are being placed in enterprise networks, massive data breaches still occur. In the recent Marriott data breach in 2018, personal information of up to 500 million people were exposed [7]. According to Marriott, the personal information that the hackers gained access included people’s names, addresses, phone numbers, email addresses, passport numbers, dates of birth, gender, Starwood loyalty program account information, and reservation information. The hackers might have stolen some of the guests’ payment card numbers and expiration dates too [7].

Many challenges have been found in ensuring data security. First, data can be stored in different medium and exist in multiple states. Data security must be ensured regardless of where it is and which state it exists. Second, the techniques used for launching cyberattacks have become more sophisticated. New threats and attacks, e.g., evasion attack and data poisoning attack [8], continue to emerge. Safeguards often lag behind in detecting and preventing these attacks. Third, cyberattacks are also becoming more organized, structured, and persistent. According to a report by the Carnegie Endowment for International Peace, state-sponsored cyberattacks are on the rise [9]. Attacks also last for a long time and attackers often have access to a compromised environment for months. Finally, cybersecurity workforce shortage continues to grow [10]. Enterprises and organizations worldwide are in need of cybersecurity professionals to fight against cybercriminals.

To protect data assets and data-driven decision

URI: https://hdl.handle.net/10125/71373
978-0-9981331-4-0

making processes, data security must be ensured. The discussions above indicate it is a challenging task. However, there are more requirements to be satisfied in data processing to ensure the intelligence developed from the process is trustworthy. This paper presents Trusted Data Processing (TDP) to achieve the goal and aims to answer three fundamental questions in TDP: 1) what are the essential requirements to achieve TDP? 2) what security mechanisms and safeguards are available to ensure TDP? 3) how to integrate TDP to practice? The contributions of the paper include, but are not limited to: 1) To the best of our knowledge, this is the first paper which presents TDP formally and discusses TDP systematically. 2) The paper summarizes the attacks targeting at data assets, their consequences, and available security mechanisms and safeguards to ensure TDP. 3) The paper provides a guidance for cybersecurity professionals to integrate TDP in practice.

The paper is organized as follows. Section 2 summarizes data characteristics. Section 3 introduces three data processing models including trusted data processing and the terms used in the paper. Section 4 presents the Trusted Data Processing model in detail using a two-step approach including data risk assessment and data risk mitigation, followed by implementation guidelines to integrate TDP in practice in Section 5. Section 6 concludes the paper.

2. Data Characteristics

The nature of data is characterized well by the 5Vs used to describe big data: volume, velocity, variety, veracity, volatility [11]. Due to the variety of data, there are many ways to classify data. According to data formats, they can be divided into structured data, unstructured data, and semi-structured data. According to their criticality, data can be classified into top secret, secret, confidential, and unclassifed. To help government agencies label critical data, NIST suggests to use Business Reference Model (BRM) to label data in 26 direct services with 98 associated information types [12].

Data may also contain sensitive information such as Personally Identifiable Information (PII), Patient Healthcare Information (PHI), Payment Card Information (PCI), and student records. Due to the sensitivity of the information, the use of the data is highly regulated. PII and PHI are protected by Health Insurance Portability and Accountability Act (HIPAA). Payment card information is under the protection of Payment Card Industry Data Security Standard (PCI DSS). Student records are protected by Family Educational Rights and Privacy Act (FERPA). In the European Union (EU), personal data is regulated by the General Data Protection Regulation (GDPR). The personal data under protection not only includes some obvious types of information like name, address, health information and IP address, but also includes information related to race or ethnicity, religion or philosophical beliefs, and sexual orientation.

Data may include critical and sensitive information. The critical and sensitive information must be secured in data processing. Stealing or disclosing critical and sensitive information is under penalty of laws. Due to the volume of data, it is not practical to have all data encrypted. Data processing might be conducted on encrypted data through homomorphic encryption [13]. However, the information which can be provided through homomorphic encryption is very limited. Safeguards must be adopted in data processing to ensure security and privacy of the data.

To develop intelligence, data needs to be processed and go through many steps such as data mining, clustering/classification, data modeling, and data summarization. The three stakeholders involved in data processing in general include data producers, data consumers, and data citizens. A *data producer* is a user interface, system or device that collects data that's relevant to an organization. Data producers are the root sources of the data. A *data consumer* is the one which uses the data. A *data citizen* is the subject of the data. In many cases, multiple systems will produce data for the same data consumer. Data consumers may create copies of data, transform it and pass it along to other systems. This can become a mess of dependencies. A single system can be both a producer and a consumer, e.g., an information broker or data broker.

Data often transforms among multiple states. It can be a hard copy of print on a desktop. It can be digital or analog signals transmitted in copper wire or optical fiber. Each state exposes very unique physical characteristics. Data often goes through multiple states when it is transmitted from one stakeholder to another. Within the perimeter of an organization, data may also exist in multiple states.

Data-driven decision making relies on the intelligence developed from the data processing. Many threats and attacks have been found targeting at data assets which may lead to false intelligence. There are three data processing models based on assumptions and objectives of data processing.

3. Data Processing Models

The three data processing models include data processing with good faith, data processing with adversaries, and trusted data processing as shown in Figure 1. We use the following terms to describe the models for the rest of the paper. Without specification, the *assets* discussed in the paper refer to data assets. Data assets are the targets for protection. *Data stakeholders* are individuals or organizations having a right, share, claim, or interest in a system or in its possession of characteristics that meet their needs and expectations. Data may stay in three *states* including data at rest, data in transit, and data in process. Data can be stolen and modified in each of the three states. An *attack* is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset. A *consequence* is the impact of an attack. A *site* is where the attack occurs. *Avenues of Attack* are means by which an asset can be impacted. An *attack surface* is the total sum of vulnerabilities that can be exploited to carry out cyberattacks. Attack surfaces can be physical or digital.

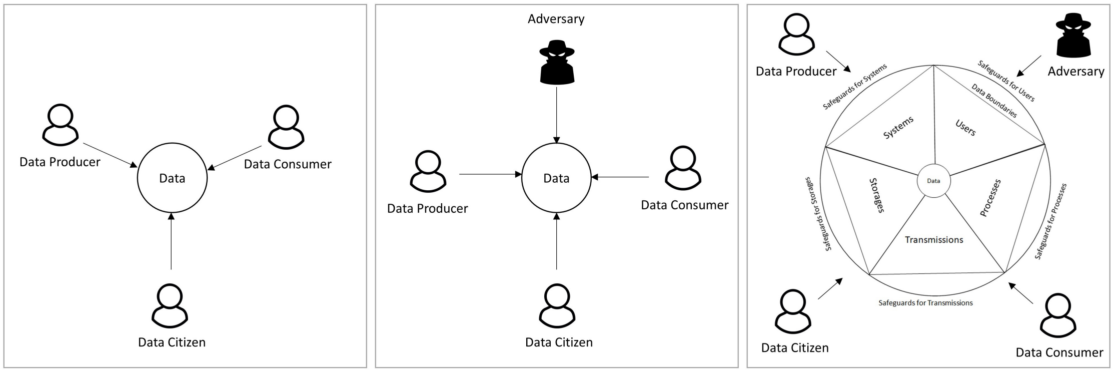
The data processing with good faith model assumes trust among stakeholders and thus assumes integrity of data in the data processing. Since this model lacks security measures to validate the integrity of the data, the model may cause havoc to the data consumers when the trust among stakeholders is violated. The use of cheques is an example of data processing with good faith. When a cheque recipient breaks the good faith with the banks, check fraud becomes criminal acts.

The data processing with adversaries model acknowledges the presence of adversaries. It requires that data producers and data consumers must be authenticated and the integrity of the data must be ensured. Data security becomes important due to the presence of adversaries. The adversary model is great for centralized data processing applications in organizations. Many safeguards have been developed and placed in enterprise networks to secure the data. However, the adversary model focuses on data within the perimeter of an organization. It is not effective in a distributed computing environment when multiple data producers are involved.

The trusted data processing model assumes the data exists in an untrusted environment and aims to develop processes to ensure the intelligence developed through the process is trustworthy. Unlike the adversary model focusing on centralized data processing, the TDP model targets at protecting data in multiple transformations in a distributed computing environment. TDP is desired in any information and intelligence systems.

Data security has been put in to a focal point in many organizations due to the cyberattacks and the data breaches occurred. There are many studies which have been conducted on data security. However, few research has been conducted on trusted data processing. Merkling defined trusted processing as a process assured by a trusted element, where use of the trusted element is based upon the principles of separation and locality [14]. In [15], Phegade et al. believed that trusted data processing is facilitated by ensuring data in insecure storage and/or traveling on insecure channels is encrypted. Data is decrypted and processed in a trusted execution environment. In [16], Peisert et al. developed a "risk profile for open science." The risk profile is a categorization of scientific assets and their common risks to science to greatly expedite risk management for open science projects and improve their cybersecurity.

It is essential to develop intelligence which can be trusted in decision-making processes. However, it is not a trivial task to achieve the goal. To achieve TDP in any data processes, it is critical to clearly identify the requirements to achieve TDP and survey available security mechanisms and safeguards to ensure TDP. The paper aims to answer the following three fundamental questions about TDP: 1) what are the



a) Data Processing with Good Faith

b) Data Processing with Adversaries

c) Trusted Data Processing

Figure 1. Data Processing Models

essential requirements to achieve TDP? 2) what security mechanisms and safeguards are available to ensure TDP? 3) how to integrate TDP to practice? The first two questions are discussed in Section 4. The third question is discussed in Section 5.

4. Trusted Data Processing

To answer Questions 1 and 2, we adopt a two-step process as shown in Figure 2. The two-step process include: data risk assessment and data risk mitigation. Data risk assessment surveys attacks and consequences on data assets. Based on the data risk profile, the requirements to achieve TDP are identified. Data risk assessment (Section 4.1) aims to answer the research Question 1. Data risk mitigation includes three steps: 1) determine security mechanism to fulfill the TDP requirements; 2) identify the challenges to be resolved to ensure the TDP; 3) place safeguards in data processing to achieve the TDP. Data risk mitigation (Section 4.2) aims to answer the research Question 2. In the end of each section in the risk assessment and the risk mitigation, use cases (Sections 4.1.4 and 4.2.4) are provided to demonstrate how risk assessment and risk mitigation can be conducted in practice.

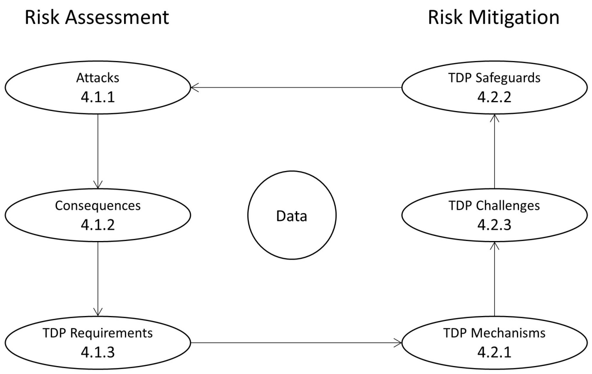


Figure 2. Trusted Data Processing: Risk Assessment and Mitigation

4.1. Data Risk Assessment

Risk assessment is a process to identify potential hazards and analyze what could happen if a hazard occurs. Data risk assessment should be conducted on all stakeholders including data producers, data consumers, and data citizens. However, many more components exist in data processing and may have impacts on TDP. In this paper, we use an *element* to describe an essential component, physical or logical, which may have an impact on data processing. An element can be an individual, a system, or an interface. Elements can be divided into the following five categories:

1. Users: such as data producers, data consumers, data citizens, adversaries.
2. Systems: including computing and communication devices.
3. Processes: a data service or process which acquires, creates, or use data.
4. Storage: such as disk, CD, flash, or piece of paper.
5. Transmission: transmission media such as cables, optical fibers, and wireless communications.

Cyberattacks usually target one or more elements in data processing. All elements together establish a data boundary around the data (Figure 1.c). Each element in the boundary must be trusted. Safeguards must be placed to secure the boundaries to protect the data.

4.1.1. Attacks Targeting at Data Assets Many attacks have been found targeting at data assets. These attacks include, but are not limited to, eavesdropping, traffic analysis, insider attack, de-anonymization attack, deep analytics attack, modification attack, replay attack, masquerade attack, repudiation attack, and Denial of Service (DoS) attack. Table 1 summarizes these attacks.

Modification attacks involve tampering data at different states. Evasion attack and data poisoning attack are two new forms of modification attacks targeting at data in process [8]. Data science heavily depends on machine learning, deep learning and other techniques to solve sophisticated problems. An evasion attack involves adversaries constantly probing classifiers with new inputs in an attempt to evade detection. Data poisoning attacks involve adversaries feeding polluted training data to a classifier, blurring the boundary between what is classified as good and bad in the adversaries' favor. Evasion attack and data poisoning attack target at computing services or processes. These attacks indicate that data security must be ensured in any state in data processing.

Deep analytics attack is another type of attack targeting at data assets using advanced analytic techniques such as clustering, classification, association rule mining to extract sensitive and valuable information. Examples of deep analytics attack include inferred information and aggregated information [17]. Inferred information is the indirection information derived from existing known data which may be linked to sensitive information such as PII. Research also

Table 1. Attacks Targeting at Data Assets

Attack	Description
Eavesdropping	also known as sniffing or snooping attack, is an incursion where an attacker passively listens to communication channels to gain access to unauthorized information.
Traffic analysis	is an attack where an adversary intercepts and examines traffic in order to deduce information from communication patterns.
Insider attack	is an attack committed on a network of computer systems by an individual who has authorized access to the network.
De-anonymization attack	is an attack where an adversary tries to recover user identities from the data available.
Deep analytics attack	is an attack where an adversary utilizes data mining and advanced analytic techniques to extract sensitive and valuable information from multiple data sources.
Modification attack	is an attack which involves modification of the data.
Replay attack	is an attack where an adversary tries to delay or resend the same packet(s) intercepted from a communication channel.
Masquerade attack	is an attack where an adversary takes false identity in order to gain unauthorized access to a data asset.
Repudiation attack	is an attack where an adversary denies that he or she performed an action or initiated a transaction.
DoS attack	is an attack where it makes a data resource unavailable for which purpose it was designed.

shows that non-sensitive data could be aggregated to reveal more sensitive information and cause identity theft. For example, the work in [18, 19] shows that 87% of Americans can be uniquely identified by five digit zip code, gender, and date of birth. However, none of them alone can significantly affect privacy.

4.1.2. Consequences of Attacks

A consequence is the negative impact of an attack [16]. The consequences of the attacks targeting at data assets include, but are not limited to, disclosure, invasion of privacy, content modification, sequence modification, timing modification, unauthorized access, malicious manipulation/forging, data rights and data ownership violation, policy violation, proprietary information loss, data loss, and Denial of Service. Table 2 summarizes these consequences.

A common consequence of attacks is data loss. Because of the value of data assets, most of cyberattacks aim to steal data from enterprises which results in data loss. Data loss includes both direct data loss and indirect data loss. Direct data loss is the loss of data stolen in a security incident. The stolen data may include users' personal information and payment card information which will have direct impact to the users. Indirect data loss is the additional information that malicious users may extract from the data using advanced data analytic techniques and the publicly available data in addition to the stolen data. The impact of data breach is usually measured by the direct data loss such as the number of users affected and the number of sensitive data records disclosed. However, it is hard to assess the indirect data loss which should also be considered in a data breach.

The attacks and their consequences are summarized in Figure 3. For example, eavesdropping attack, traffic analysis, insider attack, de-anonymization attack, and deep analytics attack may all result in unintended disclosure, invasion of privacy, proprietary information loss, policy violation, and data rights and ownership violation. The attacks and consequences figure also leads to the essential requirements to achieve the TDP.

4.1.3. Trusted Data Processing Requirements

Figure 3 indicates the key requirements which must be satisfied in TDP. For example, to prevent unintended disclosure, data should be encrypted. To ensure data rights and data ownership, transparency is required. The requirements which are essential to TDP are summarized below:

- *Data security*: Data security such as confidentiality, integrity, and authenticity must be ensured in TDP to prevent eavesdropping, modification, masquerade attacks, etc.
- *Data privacy*: User privacy should be preserved. For example, PII should not be disclosed in data processing.
- *Accountability*: The capability to trace generation and modification of data from a data producer to

Table 2. Consequences of Attacks

Consequence	Description
Unintended disclosure	not involving cyberattacks, refers to malicious or accidental disclosure of confidential or sensitive information.
Invasion of privacy	refers to the intrusion into an individual's private information.
Content modification	is a situation where an adversary changes the data content.
Sequence modification	is any changes to a sequence of message between parties including insertion, deletion, and re-ordering.
Timing modification	refers to replay or delay of any messages.
Unauthorized access	pertains to accessing or communicating or altering a resource without the system or the resource owner's consent.
Malicious manipulation/ forging	occurs when an adversary manipulates data, e.g., system log files, to forge the identification of new actions.
Data rights and data ownership violation	occurs when a user or an enterprise violates the terms of use of the data.
Policy violation	occurs when an individual or an organization violates the guidelines or policies enforced by an organization or a government agency.
Proprietary information loss	is a type of information disclosure which often results in the downfall of a company with significant economic loss.
Data loss	is any loss of data, intentionally or accidentally. Data loss may occur as the result of hardware failures, power outages, natural disasters, or cyberattacks.
Denial of Service	refers to disruption of services when data is inaccessible.

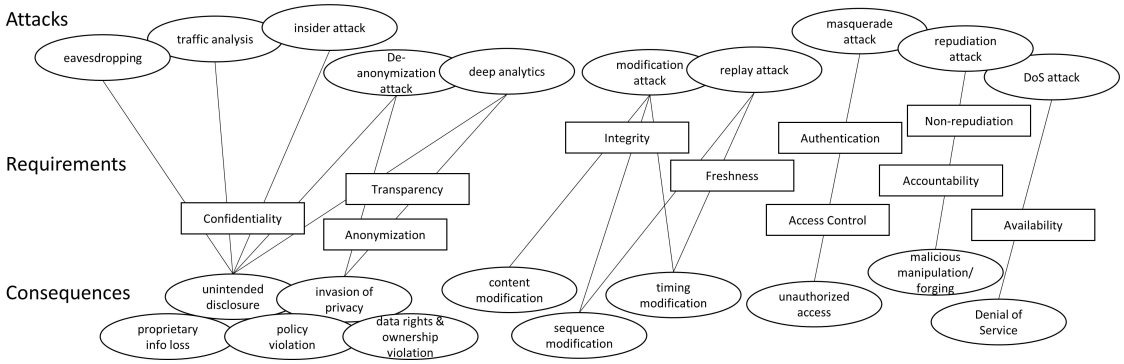


Figure 3. Attacks vs. Consequences

a data consumer is desired. Accountability helps track changes of data to prevent evasion attack and data poisoning attack.

- *Transparency*: Transparency is desired to retain data rights and data ownership. For example, the use of data must be agreed before data is collected. The data consumers must ask for user's consent if data usage is changed.

- *Distributed computing*: The requirement for security, privacy, accountability, and transparency should be achieved not only within the perimeter of an organization, but also in a distributed computing environment among multiple stakeholders.

- *Trusted elements*: The elements involved in data processing, including users, system processes, storage, and transmissions, must be trusted. A compromised element makes insider attack an easy route which may lead to massive data breach.

These requirements also lead to the services desired in TDP. Ideally, there are corresponding services such as security service, privacy service, accountability service, transparency service, distributed computing service, trusted elements service to ensure each step of the data processing to meet the TDP requirements. Most previous discussions on data processing focus on data security service. Data security service can be further identified as confidentiality, authentication, digital signatures, integrity, access control, non-repudiation, and availability [20]. However, data security alone cannot achieve TDP. Data privacy, accountability, transparency, distributed computing, and trusted elements are essential for TDP too.

Figure 4 shows a summary of the TDP services desired in data processing. If all the requirements are satisfied, it is able to verify integrity of the data, track the modification of the data, and know how exactly data is used at any point of the data processing.

4.1.4. Avenues of Attacks: A Use Case on Insider Attack Attacks targeting at data assets can occur anytime in data processing. Analysis of avenues of attacks can be conducted for each attack. The analysis includes four parts: type of the attack, consequences of the attack, where the attack occurs (i.e., site), and what is the data state when the attack occurs. Figure 5 shows an analysis of avenues of attacks on insider attack.

As shown in Figure 5, insider attacks can target at four elements in data processing, e.g., storage, transmission, data provider, and data consumer. It has consequences such as disclosure, invasion of privacy, proprietary information loss, and policy violation. According to the data state when the insider attack occurs, corresponding safeguards can be placed. By conducting analysis of avenues of attacks for all attacks, it is able to survey the attack surfaces of data assets and make plans for risk mitigation.

4.2. Data Risk Mitigation

Risk mitigation is the step taken to reduce adverse effects. The ultimate goal of TDP is to ensure the TDP requirements are satisfied at anytime during data processing. In this section, we examine the mechanisms and safeguards which can be used to ensure TDP.

4.2.1. Trusted Data Processing Mechanisms Table 3 summarizes examples of the mechanisms which can be used towards TDP services. Many of the mechanisms and safeguards depend on cryptographic operations such as encipherment, integrity, and digital signatures.

A promising mechanism to be considered in TDP is blockchian [21]. Blockchain technology has demonstrated many advantages such as distributed, stability, and trustless in digital currency such as Bitcoin. It can be adopted in data processing to provide desired services for integrity, accountability, and transparency in a distributed computing environment. While blockchain is great for tracking modification of data and establishing consent between data citizens and data consumers to maintain user data rights and data ownership, it also has limitation when used for real time applications and it requires massive storage to store blocks.

4.2.2. Trusted Data Processing Safeguards Safeguards are protective measures prescribed to meet the objectives (i.e., data security and privacy, accountability, transparency, distributed computing, and trusted elements) in TDP. Safeguards may come in different forms, from technical solutions (like encryption) to operational strategies (like plans for cyberattack incident response) to management approaches (like conducting a risk assessment).

Technical safeguards are essential for TDP services. For example, to prevent disclosure and proprietary information loss, data leakage detection and prevention solutions can be adopted [22]. However, there are many safeguards which are non-technical but are also critical for TDP. For example, to ensure a computer system is trusted, controls such as system and service acquisition and supply chain risk management must be in place. To ensure a personnel being trusted, personnel security such as screening should be used.

Many security and privacy controls are identified in [23]. These controls are divided into 20 control families and can be classified into three categories in general: controls for security, controls for privacy, and controls for both security and privacy. Safeguards should also be placed to support accountability, transparency, distributed, and trusted elements. There is no single safeguard which can be used to provide all the services essential in TDP. It is also important to note that a safeguard can be used to achieve multiple objectives in TDP. Figure 4 shows examples of safeguards which can be adopted in TDP.

4.2.3. Trusted Data Processing Challenges TDP is desired in any intelligence and information systems. The number of data breaches occurred indicate it is a complicated issue. There are many challenges which need to be addressed to achieve TDP.

- *Extremely large attack surface*: Many elements including users, systems, processes, storage, and transmissions are involved in data processing. Malicious users can select any element as a target and experiment each avenue of attacks until one gets through. To secure each element and reduce attack surface is not a trivial task.

- *Privacy at risk*: The advancement of Internet of

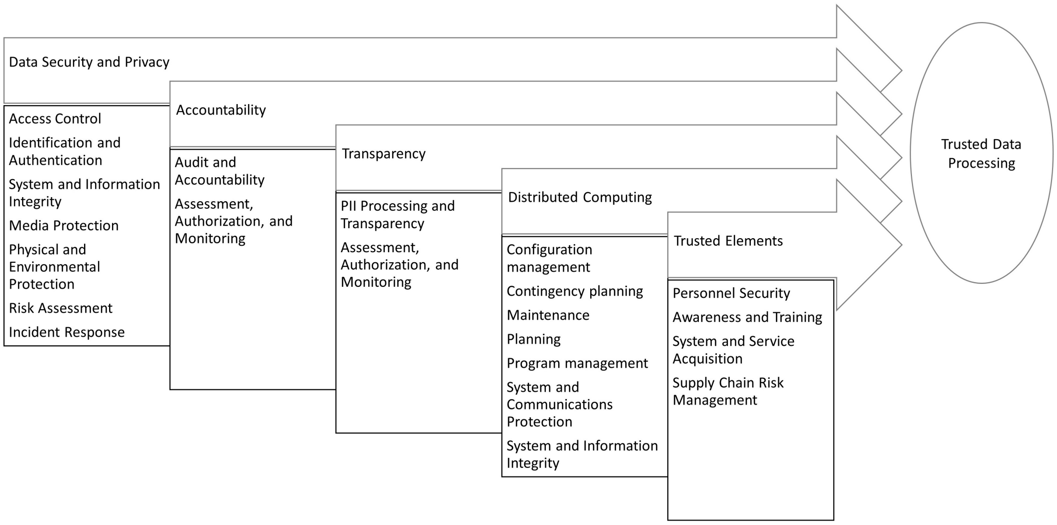

Data Security and Privacy
Access Control
Identification and Authentication
System and Information Integrity
Media Protection
Physical and Environmental Protection
Risk Assessment
Incident Response
Accountability
Audit and Accountability
Assessment, Authorization, and Monitoring
Transparency
PII Processing and Transparency
Assessment, Authorization, and Monitoring
Distributed Computing
Configuration management
Contingency planning
Maintenance
Planning
Program management
System and Communications Protection
System and Information Integrity
Trusted Elements
Personnel Security
Awareness and Training
System and Service Acquisition
Supply Chain Risk Management
Trusted Data Processing

Figure 4. Trusted Data Processing Requirements and Safeguards

Table 3. TDP Services and Mechanisms

TDP Service		Mechanisms
Data Security	Confidentiality	encipherment, routing control
	Integrity	encipherment, digital signatures, data integrity
	Authentication	encipherment, digital signatures, authentication exchange
	Access control	access control
	Non-repudiation	digital signatures, data integrity, notarization
	Availability	data integrity, authentication exchange
Data privacy		encipherment, traffic padding
Accountability		digital signatures, data integrity, authentication exchange, notarization
Transparency		digital signatures, access control, authentication exchange
Distributed		digital signatures, data integrity, authentication exchange
Trusted element		notarization

Things (IoT) and deep data analytics makes user privacy at risk. When everything is connected, e.g. Internet of Everything (IoE), without regulations and polices, preserving user privacy becomes almost an impossible task.

- *Interoperability issues*: Accountability and transparency are important services to achieve TDP. Within the perimeter of an organization, centralized solutions can be found. However, a solution in a distributed environment to ensure accountability and transparency requires interoperability among multiple information systems among multiple organizations. For example, a distributed key management system to ensure accountability and transparency is required.

- *Big data challenges*: Big data presents many challenges for TDP. Traditional cryptographic operations are essential to protect data security such as confidentiality, integrity, and authentication. However, the volume of big data raises a major concern on performance when applying cryptographic operations such as encipherment, digital signatures, and data integrity on the targeted data.

- *Emerging new threats and attacks targeting at data assets*: Many threats and attacks target at data at rest and data at transmission. Recent research also found attacks targeting at data in process [8]. Artificial Intelligence and many other safeguards such as intrusion detection and malware detection utilize machine learning to process data. It is important to integrate safeguards to prevent threats and attacks for data in process too.

- *Trusted elements and the weakest link*: TDP

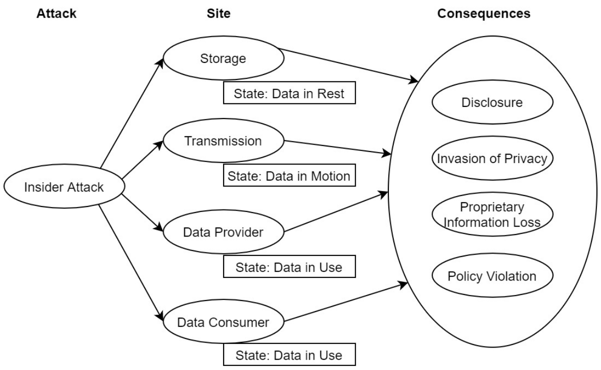


Figure 5. Avenues of Attacks: A Use Case on Insider Attack

requires each element in the process being trusted. A trusted element indicates each component of the element being trusted. This alone is a very challenging issue. Further, people are often the weakest link among all the elements. A data process cannot be trusted even with just one untrustful element.

- *More than technical solutions*: Many safeguards have already been adopted in data processing. The places of safeguards and technical solutions may give people false feeling of security. The technical solutions alone are not sufficient to ensure TDP. Technical solutions must be combined with non-technical solutions and organized in a more systematic and strategic way in TDP.

4.2.4. Risk Mitigation: A Use Case on Insider Attack Analysis of risk mitigation can be conducted on each attack. Safeguards should be placed on each element and in each step of data processing to ensure TDP. In Section 4.1.4, we demonstrated an analysis of avenues of attacks on insider attack. Using the avenues of attacks figure, analysis of risk mitigation can also be conducted. Figure 6 shows an analysis of risk mitigation for each element as identified in Figure 5 on insider attack.

As shown in Figure 6, to mitigate risk associated with insider attack, safeguards should be applied on each element at different states of the data. Skipping an element or lack of safeguards in a state will lead to possible vulnerabilities in TDP. Similar analysis can be conducted on all the other attacks.

5. Trusted Data Processing Guideline

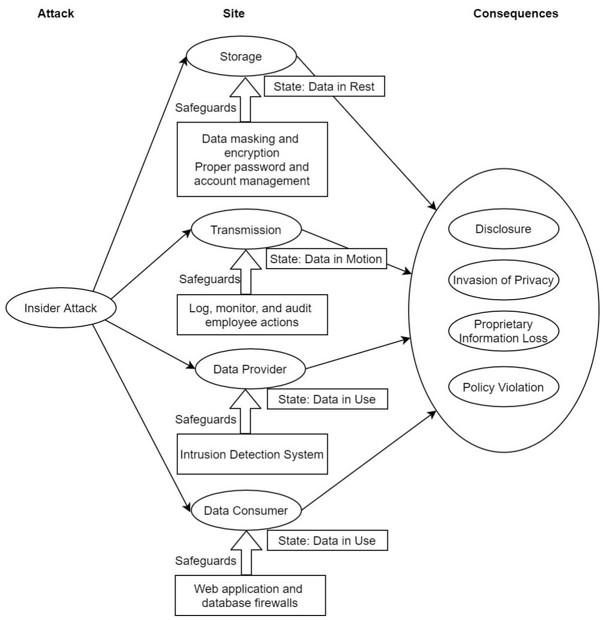


Figure 6. Risk Mitigation: A Use Case on Insider Attack

NIST Cybersecurity Framework provides a general guidance which can be adopted by any organization to manage their cybersecurity risks [24]. TDP can be integrated with NIST Cybersecurity Framework Core Functions, i.e., identify, protect, detect, respond, recover, to help organizations mitigate security risks on data assets.

- *Identify*: The target to protect is data assets. Many threats and attacks have been found targeting at data at rest, data in transition, and data in process. Their consequences have been discussed. Based on the attacks and their consequences, services to ensure TDP are identified. These desired services include data security, data privacy, accountability, transparency, distributed computing, and trusted elements.

- *Detect*: Many safeguards can be utilized to detect violations of TDP [22]. The violations should be monitored include not only violations of data security and privacy, but also violations of other TDP requirements.

- *Protect*: TDP services such as data security, data privacy, accountability, transparency, distributed computing, and trusted elements should be retained from end to end in the process. A Defense-in-Depth approach can be used to systematically place safeguards.

- *Respond*: Appropriate actions should be taken when violations of TDP are detected. For example, when data integrity is violated, session termination should be conducted.

- *Recovery*: Using the Attacks and Consequences chart, plans can be developed to restore the desired service when a cyberattack is detected.

6. Summary

This paper introduced Trusted Data Processing and addressed three fundamental questions in TDP. Based on the attacks targeting at data assets and their consequences, the paper identified six essential requirements, including security, privacy, accountability, transparency, distributed computing, and trusted elements, to achieve TDP. For each TDP requirement, corresponding service is required to meet the requirement. For each service, the paper also identified available security mechanisms and safeguards to implement the service. Many controls have been in place for data security and privacy. More safeguards need to be developed to ensure accountability, transparency, distributed, and trusted elements. Ensuring TDP in each step of the data processing is not a trivial task. There are many challenges. These challenges include, but are not limited to, extremely large attack surface, privacy at risk, interoperability issues, big data challenges, new emerging threats and attacks, trusted elements and the weakest link, and more than technical solutions. To integrate TDP in practice, the paper suggested a five-step process using the NIST Cybersecurity Framework. Our future work includes: 1) conduct risk assessment and risk mitigation on each attack targeting at data assets as identified in Table 1; 2) develop practical assessment methods for Trusted Data Processing based on its requirements.

References

[1] McKinsey Global Institute, "The age of analytics: Competing in a data-drivel world," Tech. Rep. December, 2016.

[2] D. Reinsel, J. Gantz, and J. Rydning, "The digitization of the world," tech. rep., IDC, 2018.

[3] J. Short and S. Todd, "What's your data worth?," *MIT Sloan Management Review*, vol. 58, no. 3, p. 17, 2017.

[4] Netwrix, "2020 netwrix it trends report," tech. rep., Netwrix, Irvine, CA, 2019.

[5] Gartner, "Gartner forecasts worldwide information security spending to exceed $124 billion in 2019," aug 2018.

[6] C. Riggs, *Network perimeter security: building defense in-depth*. CRC Press, 2003.

[7] G. Seena, "The Marriott data breach," December 2018.

[8] J. Su, D. V. Vargas, and K. Sakurai, "One pixel attack for fooling deep neural networks," *IEEE Transactions on Evolutionary Computation*, vol. 23, no. 5, pp. 828–841, 2019.

[9] D. S. Hermiyanty, Wandira Ayu Bertin, "The cyber threat landscape - confronting challenges to the financial system," Tech. Rep. 9, 2017.

[10] The White House, "Executive order on america's cybersecurity workforce," 2019.

[11] NIST, "Big data interoperability framework: volume 4, security and privacy version 3," tech. rep., National Institute of Standards and Technology, 2019.

[12] K. M. Stine, R. L. Kissel, W. C. Barker, A. Lee, J. Fahlsing, and J. Gulick, "Guide for mapping types of information and information systems to security categories (2 vols.)," tech. rep., National Institute of Standards and Technology, 2008.

[13] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?," in *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*, pp. 113–124, 2011.

[14] R. Merkling, H. Fieres, and K. Klemba, "Method and apparatus for trusted processing," Nov. 24 1998. US Patent 5,841,869.

[15] V. Phegade, N. K. Jain, and J. Walker, "Trusted data processing in the public cloud," Aug. 25 2015. US Patent 9,118,639.

[16] S. Peisert, V. Welch, A. Adams, R. Bevier, M. Dopheide, R. LeDuc, P. Meunier, S. Schwab, and K. Stocks, "Open science cyber risk profile (oscrp)," 2017.

[17] R. K. Nepali and Y. Wang, "Sonet: A social network model for privacy monitoring and ranking," in *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops*, pp. 162–166, 2013.

[18] P. Golle, "Revisiting the uniqueness of simple demographics in the US population," in *Proceedings of the 5th ACM workshop on Privacy in electronic society*, WPES '06, pp. 77–80, ACM, 2006.

[19] L. Sweeney, *Uniqueness of Simple Demographics in the U.S. Population, LIDAP-WP4*. Carnegie Mellon University, Laboratory for International Data Privacy, 2000.

[20] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Pearson, 7th ed., 2016.

[21] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[22] A. Shabtai, Y. Elovici, and L. Rokach, *A survey of data leakage detection and prevention solutions*. Springer Science & Business Media, 2012.

[23] NIST, "Nist special publication 800-53 rev. 4 security and privacy controls for information systems and organizations," tech. rep., National Institute of Standards and Technology, 2020.

[24] NIST, "Framework for improving critical infrastructure cybersecurity," tech. rep., National Institute of Standards and Technology, 2018.