ISSN 2278-3091
Volume 8, No.1.4, 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse8081.42019.pdf
https://doi.org/10.30534/ijatcse/2019/8081.42019

Unified and Stable Privacy Model

Mohamed E. Fayad[1], Gaurav Kuppa[1], David Hamu[2]
[1]Department of Computer Engineering, Charles W. Davidson College of Engineering, San Jose State University, San Jose, CA, USA, [1]m.fayad@sjsu.edu, gaurav.kuppa@sjsu.edu
[2]Liberty Consulting, Mesa, AZ, USA, dave.hamu@gmail.com

ABSTRACT

In the information age, people can access any information momentarily. With such power, internet providers and technology companies bear the responsibility for securing information as per the user's granted permissions. This paper will present a unified and stable pattern of privacy across all domains and present a stable model for privacy for unlimited applicability. The idea of this paper is to create stable functional and nonfunctional requirements and design the right to privacy to be used. While the functional requirements determine the purpose and the technical details of the system; nonfunctional requirements identify conceptual criteria of an effective system. We employ software stability model (SSM) versus the traditional model (business as usual) to define these requirements. We then employ a weighted study will then to compare the functional and non-functional requirements of privacy. The findings of this work are that (1) the Stable Privacy Model can be applied to all conceivable scenarios whereas the traditional model (TM) is limited to a single-use model that cannot be repurposed. Additionally, (2) the paper establishes the true functional and nonfunctional requirements of Privacy, and (3) creates a stable pattern language with unification, reusability, and unlimited applicability.

Key words: Privacy, Stable, Pattern, TM, SSM

1. INTRODUCTION

Privacy is the ability for a person to remove one's information or person from a compromising state. Recently, the right to privacy has been under the spotlight with increased information sharing tools. Large corporations have enormous power to collect and potentially abuse or compromise customer and user information. Moreover, these corporations do not face any consequences for privacy infringement other than lowered public sentiment, because they are effectively protected by obtuse and even vague privacy policies. Similarly, the government's surveillance powers create many privacy concerns because privacy is vital to most other human rights. To effectively identify solutions to the many privacy-related problems, we must establish a clear understanding of privacy across all domains and contexts. Through a universal understanding of privacy, the core principles of privacy will be defined. It is crucial to analyze both universally applicable facets of privacy and foundational core principles of privacy in order to arrive at proper and effective solutions to privacy and its issues across the various domains that impact privacy considerations both at home and globally.

Within the technology domain, the Privacy Stable Analysis Pattern uses the guiding principles of stable software patterns to create an architecture that describes a comprehensive and domain-independent privacy model. The lack of a universal understanding of the right to privacy is troublesome for many reasons. Beyond creating a unified understanding, the stable analysis pattern of the right to privacy define the essential properties of privacy. Concepts of Enduring Business Themes (EBTs) and Business Objects (BOs) will be applied to these stable analysis patterns. The EBTs and BOs form the core knowledge principles of privacy in such a way that the stable analysis pattern can be used for any instance of privacy [1]-[3]. As a result, a unified set of knowledge will enable a solid model for privacy to be effectively analyzed and implemented across many domains.
This paper is organized by 5 major sections: Section 2 provides scenarios of privacy in use; Section 3 describes the contexts of Privacy; Section 4 illustrates corresponding traditional models; Section 5 portrays a stable, unified model with EBTs and BOs based on nonfunctional requirements; Section 6 details additional scenarios of Privacy; Section 7 shows the applicability of Privacy via Stable Analysis Patterns; Section 8 details a weighted comparison between the traditional and stability models; Section 9 presents further discussion about privacy; and Section 7 presents a conclusion.

2. THE PROBLEM

With the inevitability of information sharing and communication, the technologically-modern world has been more transparent than ever. Coincidentally, this has lead to the rise of the vulnerability of information and lack of data privacy. Historically, international decelerations of political and human rights [4] have stated privacy to be instrumental to humanity. It follows that privacy needs to be a core issue of debate and instrumental part of all future innovation. The debate about privacy raises the vital question of the social responsibility of those who create technological platforms and information sharing mechanisms. The prerequisites for fruitful debate and implementation of privacy is to have a clear understanding of how privacy operates from all perspectives. Unfortunately, there is no clear, concise

definition of what privacy is. More specifically, all definitions of privacy struggle to cohesively describe privacy and properties of applied privacy through its functional and non-functional requirements, respectively. Privacy encompasses the right to be let alone, or freedom from interference or intrusion [5]. According to the legal system, "the right of privacy must be balanced against the state's compelling interests. Such compelling interests include the promotion of public morality, protection of the individual's psychological health, and improving the quality of life." This distinction and ambiguity in the application become a problem when debating privacy laws across applications. Clearly, there is no unified and applicable definition for Privacy, and this paper uses functional and non-functional requirements to illustrate that.

3. CONTEXT

The Privacy design analysis can be applied to scenarios across a vast spectrum. Privacy is prevalent in healthcare, technology, art, science, political, etc. industries and can lead to many different complications. Regardless, all privacy has the same requirements and common key patterns that are instrumental in retaining privacy. It is important to analyze its patterns to portray and break down Privacy. In the following, we will illustrate some of the endless possible scenarios. In the process of doing so, it will become increasingly clear that Privacy has a common set of patterns.

Scenario #1: **Two Factor Authentication**

The Wells Fargo (AnyParty) application allows its customers (AnyParty) to access important bank information and perform basic tasks related to their accounts from their phone (AnyMedia). Obviously, Wells Fargo stores a lot of personal information about its customers. To preserve customer trust and privacy (AnyReason) and abide by its privacy policy (AnyPolicy), Wells Fargo implements security measures (AnyRule) through a rigorous two-factor authentication procedure (AnyMechanism) that uses a third-party application (AnyResource) to confirm the user's identity. These measures are backed up. Wells Fargo's security system influences the criteria that it sets to ensure that user information is secure (AnyCriteria). Furthermore, the information (aka PII - Personally Identifiable Information; and NPI - Non-Public Information) must not be lost or released into the public domain as a result of error or malice. In doing so, all past, current, and future customers are ensured of their privacy and can expect their information to be entirely secure.

Scenario #2: **New Privacy Laws**

Soon after the Facebook (AnyParty) – Cambridge Analytica (AnyParty) data scandal (AnyReason), the European Union instigated a set of laws called the General Data Protection Regulation (GDPR) (AnyPolicy). These laws (AnyMechanism) attempted to ensure that citizens would have greater control over their personal data (AnyReason) in cyberspace. These regulations must be abided to by all companies (AnyParty) who require users to disclose private data (AnyMeasure). Specifically, each company must employ a data protection officer (AnyResource), report data breaches immediately (AnyResource), etc. Failure to comply with these regulations results in vast fines and which may include civil and even criminal penalties.

4. TRADITIONAL PRIVACY MODEL

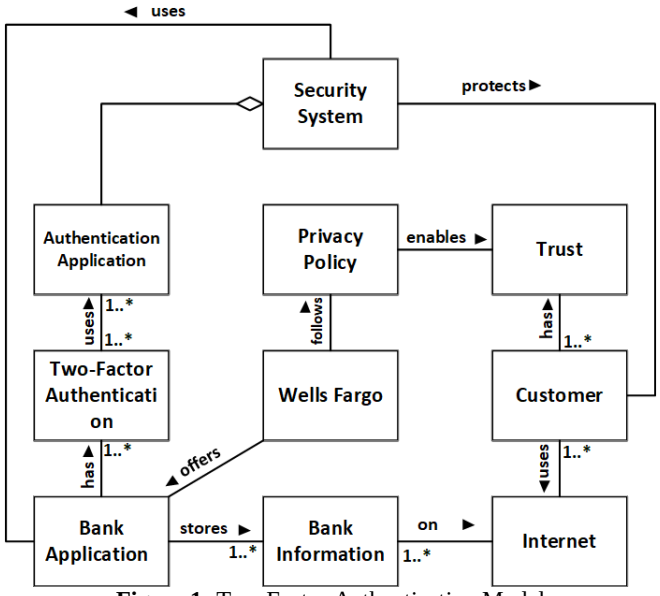

Figure 1: Two Factor Authentication Model

The Traditional Privacy Model is an unstable, inflexible, non-adaptive architecture that does not fulfill usage conditions that differ from one scenario to the other. [6], [7] It can only fulfill the current requirement in hand, without considering any type of future modifications or alterations (As shown in Figure 1.). In the diagram given below, certain instances of customer records are provided, which when subjected to changes and alterations may render the entire architecture useless and become redundant.

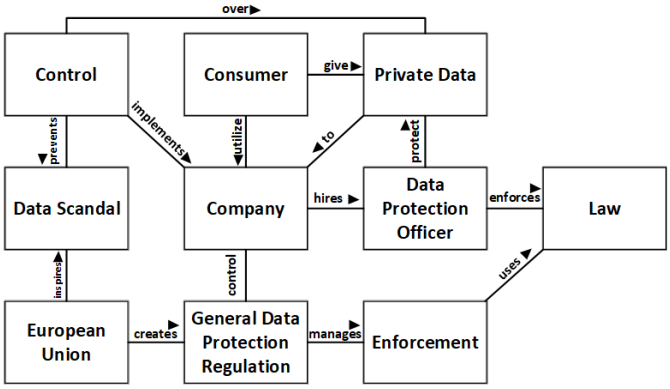

Figure 2: New Privacy Laws Model

A traditional model obscures the actual goal of privacy. There is no clarity of the problem space, and therefore, no clear solution space. The privacy concept needs to be modeled through the software stability paradigm in order to achieve stability, consistency, reusability, and reliability.

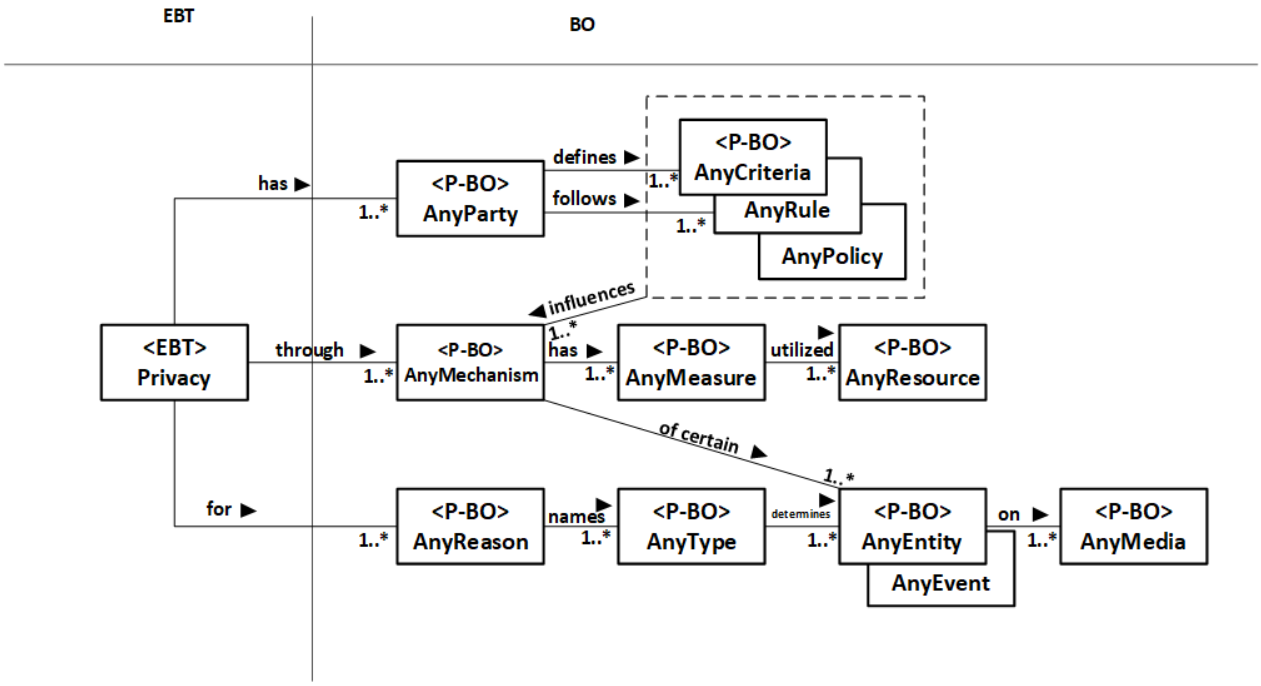

Figure 3: Privacy Stable Analysis Pattern [8]

5. STABLE PRIVACY MODEL

Figure 3 depicts a stable privacy model that is generated based on Softwre Stability Model which consists of an Enduring Business Theme (EBT), Business Objects (BOs) and will be attached to Industrial Objects (IOs) as application objects.

The functional requirements for the privacy model are:

Object	Definition
1. AnyParty	The legal user of the system, which may be a person, organization, country or political party
2. AnyCriteria	A specification for judging, but it can also be a prerequisite for an achievement
3. AnActor/Any Party	Defines the criteria for the creation of something
4. AnyRule	Some rules to be implemented
5. AnyPolicy	Some constraints to be followed for a particular action
6. AnyMechanism	A process that has been setup to accomplish a particular goal
7. AnyMeasure	Some steps for following a protocol
8. AnyResource	Something that is useful in doing a task)
9. AnyReason	Some cause for action
10. AnyType	A category of things distinguished by some common characteristic or quality
11. AnyEntity	Something that can be perceived, known or inferred to have its own distinct existence, it may be living or non-living, and helps or is the result of creation)
12. AnyEvent	Something that has happened or might happen, due to which creation is done, or needs to be done
13. AnyMedia	Feedback from a person or a party can be collected on any kind of media. It can be used to record any kind of log

The non-functional requirements are:

1. Right – Privacy should be a right for all that want it. As the basis for individual choice, privacy enables all other human rights. Freedom of speech, freedom of religion, etc. are only observed if one is able to use these freedoms if given the ability to have privacy.
2. Protection- It should provide protection from those who are seeking to create vulnerabilities. Privacy, as a concept, should be easy to deploy to maintain protection. In addition, a party that wants to maintain privacy should be able to trigger mechanisms through which privacy is enforced.
3. Safety – Privacy should be able to retain the safety of AnyParty through AnyMechanism. It should be enough

to hold onto the various factors. Safety is a main component of Privacy because it prevents AnyParty from being in harm's way as a result of a leak of information that could be determinant to their health. As such, no one should be able to intrude and access the information without authorization.

4. Control – When Privacy is achieved, AnyParty will feel a sense of control over their possessions and the experiences they had. This sense of control enables stability for AnyParty and confidence that they can exercise control over their future. Especially in a world of uncertainty, it is extremely important for people to have a sense of control over their life and their private information.
5. Dignity- Privacy allows the ability to have a dignified, respectable sense of living. This dignity should persist throughout any interaction a person who can protect themselves from external invasion is able to proceed through their lifestyle with their rights being respected.
6. Confidentiality – Privacy is retained through AnyRule and its accompanying confidentiality agreements. Confidentiality is a hallmark of privacy because it defines the specifics of the boundaries and reaches of privacy. In practice, privacy is executed through abiding by these set of rules.

The stable privacy model as presented in Figure 3, presents a number of features that are unique to the stable software methodology. The core component of the model is privacy, which denotes the need to maintain secrecy. An actor or a party needs to maintain privacy for some pre-defined reasons, which eventually decides the basic aspects of secrecy and its application. An actor or party should be present to experience the concept of privacy and secrecy, and he/she may set up the perimeter for secrecy based on some pre-defined criterion. A person or an animal may decide to set the terms for implementing the basic aspects of privacy. Eventually, privacy is manifested by enforcing secrecy, confidentiality, and results in protection from public scrutiny of the actor who is covered by privacy.

Privacy could be enforced in many ways, and the party who wants privacy may choose to alter criteria that are needed to enforce privacy. In fact, an actor may choose to maintain secrecy depending on existing need and requirement. In other words, the actor might wish to tweak and calibrate requirements to adjust the level of privacy. The actor must set some rigid rules that can be implemented very easily to maintain or propagate privacy. To promote privacy, an actor should also set some constraints (policies) to enable a particular plan of action. Once the rules are in place, the actor may need to initiate some processes (mechanism) to achieve the ultimate goal (in this case, privacy). The actor may need to undertake some measures or steps while he/she can use any type of resources that they feel are important for the assigned task to follow the protocols set for the process. Seeking privacy is due to some specified reasons, while events that are out of reach may force a party to seek or enforce privacy. Eventually, the feedback in response to privacy enforced could be recorded in various formats, logs, and media.

Table 1: Applicability of 5 Scenarios

EBT	**BOs**	**App-1 – Apple Pay Data Privacy**	**App-2 – Due Process**	**App-3 – Financial Privacy**	**App-4 – Medical Records Privacy**	**App-5 – Freedom of Speech**
Privacy	AnyParty	Apple Phone Customer	United States of America Citizens Lawyer	Bank Account Owner	Hospital Patient	United States of America Citizens
	AnyCritera/ AnyRule/ AnyPolicy	Privacy Policy	4th Amendment	Confidentiality	Health Insurance Portability and Accountability Act	1st Amendment
	Any-Mechanism	Encryption	Justice Process	Insurance	Law Enforcement	Police
	AnyMeasure	Protection Rate	Jury	Technology	Accountability	Censorship
	AnyResource	SHA-256	Court	Money	Nurse	Court
	AnyReason	Legality	Protection	Personal	Secure	Justice
	AnyType	Mobile	Legal	Monetary	Medical	Human Right
	AnyEntity /AnyEvent	Silicon Valley	U.S. Constitution	FDIC	Appointment	U.S. Constitution
	AnyMedia	iPhone	Paper	Bank Statement	Record Keeping	Paper

6. APPLICABILITY

Note that the patterns will remain very similar across all applications. This is purposely designed as such to standarize the core knowledge of Privacy to enable the ability to build numerous applications.

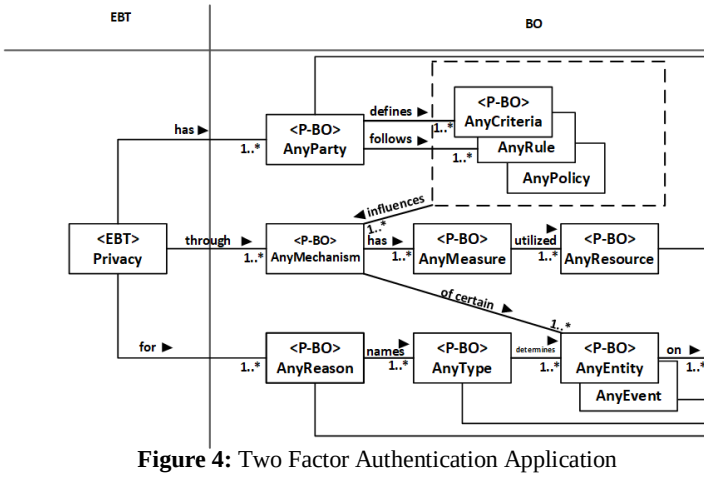

Figure 4: Two Factor Authentication Application

Application 1 –Two Factor Authentication Model

In reference to Scenario 1, we construct a Stable Analysis Pattern below.

Application 2 – New Privacy Laws Model

In reference to Scenario 2, we construct a Stable Analysis Pattern below.

7. COMPARATIVE STUDY

7.1 Weighted Comparative Study

Both the traditional and stable models documented above may be compared based on privacy non-functional requirements. The total score of 100 points will be assumed and split based on the following factors: Right and Protection (20 points each) and Safety, Control, Dignity, and Confidentiality (15 points each. The results of the analysis of both models are shown in Table 2.

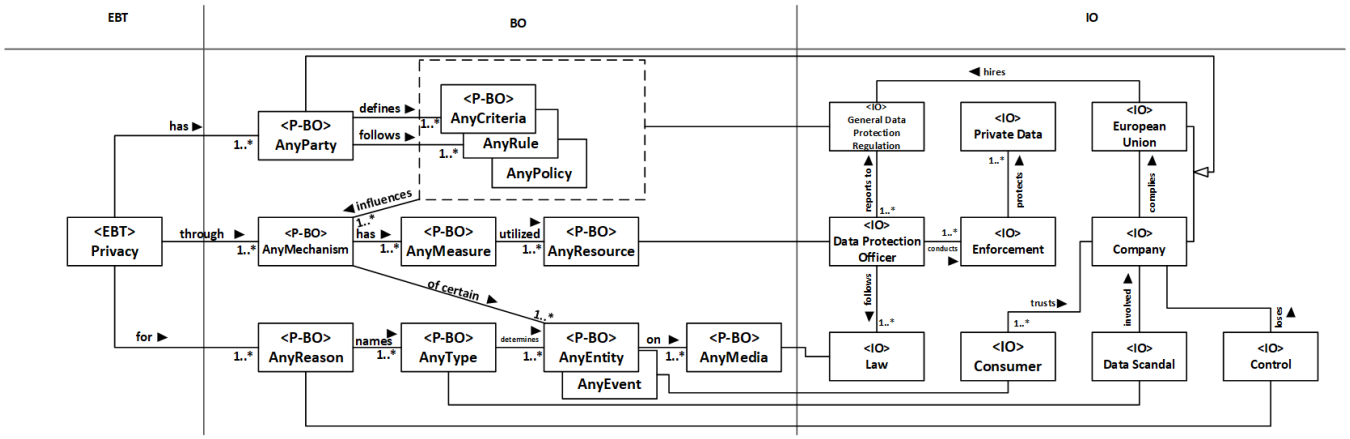

Figure 5: New Privacy Laws Application

Table 2: TM vs SM Weighted Comparative Study

Criteria	% Weight	Description for TM	Weight of TM	Description for SSM	Weight of SSM
Right	20	The TM does not always specify what Right is in question or potentially violated. The lack of consistency is troubling.	12	The SSM clearly states what AnyPolicy applies to the scenario that is being modeled.	20
Protection	20	The TM does not display how it will protect the Privacy of the actors, for any scenario.	10	The SSM clearly uses AnyMechanism in order to show the way Privacy will be executed.	20
Safety	15	The TM can display elements of safety; however, the high dependence within the structure shows the volatility	9	The SSM shows have a lesser dependence between classes, and the relations are spread out more evenly,	18

		of the system.		allowing it to be safe even against malfunctions.	
Control	15	The TM does not show a structure of control, such that it will retain Privacy.	3	The SSM shows an entire structure via the core knowledge of Privacy [9]. This will act as the backbone of all Privacy scenarios.	15
Dignity	15	The TM does not portray the humanity of the actors within its modeling.	8	The SSM has the AnyReason pattern to convey the dignity and humanity of AnyParty, but it is not very clear that AnyReason is meant to serve this purpose.	10
Confidentiality	15	The TM is not effective at conveying the extent to which Privacy is retained.	6	The SSM shows AnyRule and AnyCriteria that are in consideration when retaining confidentiality.	11
Total	100		48		94

7.2 Measurability

A. Quantitative Measurability

For this section, there is one qualitative and one quantitative metric that is used to measure the two models. They are explained below:

Quantitative: # of classes with 3 or more client classes

This metric measures how many classes are associated with more than two classes. The formula for this is given as follows:

C3P = TC - (C2 + C1 + CS)

C3P - Number of Classes with 3 Plus Associations to other classes
TC - Total amount of Classes
C2 - Number of Classes with 2 Associations to other classes
C1 - Number of Classes with 1 Association to another class
CS - Number of Classes that only associate with themselves

Traditional Model #1:
TC = 10
C2 = 4
C1 = 0
CS = 0
C3P = 10 - (4 + 0 + 0)
C3P = 6

Traditional Model #2:
TC = 10
C2 = 3
C1 = 0
CS = 0
C3P = 10 - (3 + 0 + 0)
C3P = 7

Stable:
TC = 11
C2 = 3
C1 = 3
CS = 0
C3P = 11 – (3 + 3 + 0) = 5

As a result, the stable model has fewer classes that are associated with 3 or more other classes. This means that the classes in the stable model don't need to interact as much with each other and the system can still work. The more a class uses another class, the more it may depend on that class to perform.

B. Qualitative Measurability

The qualitative measurement metric used to compare stable and traditional models is applicability. Traditional models cannot extend beyond a single scenario because each model is specific to a particular application. In conjunction with the application-specific patterns, traditional models cannot be applied to other application contexts because each traditional model is specifically tailored to a single use case. On the other hand, the stable model defines a core knowledge architecture that defines the common goal for all applications of Privacy. This core knowledge is defined in a way that it can define the vital aspects of Privacy, as defined by the goal and non-functional requirements. Therefore, the generality of the stable model lends it to be able to be applied to all applications of Privacy.

8. DISCUSSIONS AND ANALYSIS

8.1 Abstraction

The stability model for privacy is far more stable, superior, complete and flexible for a wide range of applications. Similarly, this model and its dynamics are easy to understand and comprehend even by inexperienced pattern developers. Conversely, a traditional model although easy to understand, is not fully accurate and its approach may fail to address universality of domains and application scenarios that might lie outside the periphery **of** the core of the problem, i.e., the concept of privacy.

8.2 Application

The Privacy, Stable Pattern is accurate, flexible and reusable with an ability to extend its advantages to a diverse number of applications where the concept of privacy is involved. Privacy can exist in different domains including software science, politics, medicine, personal and professional areas, business and in those areas where someone one needs privacy to remain secretive and stay in-cognition.

9. CONCLUSION

Ultimately, the Privacy Stable Model offers practical solutions to common problems that usually occur while creating a traditional pattern which is highlighted in this paper. This model is stable and applicable to a number of domains that eventually makes it a far superior pattern making technology, when compared to the model designing that uses traditional technology. Using a combination of EBTs, BOs and IOs make this pattern extremely stable, reusable, adaptive and robust; in essence, its stable architecture also makes it sturdier to immediate or any future changes and modifications that demand reorientation and redesigning of the pattern right from the start.

REFERENCES

[1] M.E. Fayad and A. Altman. **An Introduction to Software Stability,** *Communications of the ACM,* Vo. 44, No. 9, September 2001, pp 95-98. https://doi.org/10.1145/383694.383713

[2] M.E. Fayad. **Accomplishing Software Stability**, *Communications of the ACM,* Vo. 45, No. 1, January 2002, pp 95-98. https://doi.org/10.1145/502269.502308

[3] M.E. Fayad. **How to Deal with Software Stability,** *Communications of ACM*, Vol. 45, no. 4, Apr. 2002, pp. 109-112. https://doi.org/10.1145/505248.505278

[4] **Universal Declaration of Human Rights**. NY, NY: United Nations, 2017.

[5] Westin, Alan F. ***Privacy and Freedom***. New York: Atheneum, 1970.

[6] Nyisztor, Karoly, and Monika Nyisztor. ***UML and Object-Oriented Design Foundations: Understanding Object-Oriented Programming and the Unified Modeling Language*.**

[7] Sommerville, Ian. ***Software Engineering***. 10th ed. Boston: Pearson, 2016.

[8] M.E. Fayad, **Stable Design Patterns for Software and Systems**. Auerbach Publications, July 2017 , 600 pages https://doi.org/10.1201/9781315119366-15

[9] M.E. Fayad, H. Sanchez, S. Hegde, A. Basia, and A. Vakil. **Software Patterns, Knowledge Maps, and Domain Analysis**. Auerbach Publications, December 2015 , 422 pages https://doi.org/10.1201/b17771