Preprint: 7th IEEE International Conference on Big Data Security on Cloud (BigDataSecurity 2021)

Automated Compliance of Mobile Wallet Payments for Cloud Services

Ankur Nagar
Information Systems
University of Maryland, Baltimore County
Baltimore, MD, USA
anku2@umbc.edu

Lavanya Elluri
Information Systems
University of Maryland, Baltimore County
Baltimore, MD, USA
lelluri1@umbc.edu

Karuna Pande Joshi
Information Systems
University of Maryland, Baltimore County
Baltimore, MD, USA
karuna.joshi@umbc.edu

***Abstract*—Mobile payments are on the rise, and as their popularity is emerging, providers must adhere to security regulations to ensure consumer confidence. There is currently no single regulation specific to mobile wallets, so existing banking transactions are used to secure mobile payment transactions. These financial regulations are large textual documents and require significant manual effort to comprehend and ensure compliance adherence. Thus, it is difficult for both the consumers and providers to understand which specific rules in these regulations apply to their mobile wallet transactions. We have created an integrated knowledge representation of the four main banking regulations that apply to mobile payment Electronic Funds Transfer Act (EFTA), Truth in Lending Act (TILA), Gramm-Leach-Bliley Act (GLBA), and Payment Card Industry Data Security Standards (PCI-DSS). In this paper, we present our framework in detail along with the qualitative and quantitative measures that were used to validate the design against the policies of six major vendors that deal with mobile payments. Our integrated mobile payment knowledge graph, which is available in the public domain, can be used by practitioners to automate mobile wallet transaction compliance in their organization.**

***Index Terms*—Mobile Wallets, PCI DSS, Regulations, Semantic Web, OWL, SPARQL, Compliance, Finance.**

I. Introduction

Digital mobile wallets are transforming the world of consumer payments and commerce. They are the computer software applications that store and transmit payment authorization data for one or more credit, debit, gift card accounts. The consumer loads the payment account data into the digital wallet, which functions as a payment device for the selected account, transmitting the data to merchants to authorize payment. By storing payment authorization data, digital wallets function analogously to physical wallets that contain multiple payment cards used to transmit payment authorization data [1]. Mobile payment is commonly defined as "the process of using a hand-held device to pay for a product or service, either remotely or at a point of sale" [1] [2].

To ensure high consumer confidence in digital wallets, providers of these services must ensure strict data security and privacy. One way to ensure that is to comply with rules listed in data protection regulations. There is currently no single regulation specific to mobile wallets, so existing regulations for banking transactions are being used to secure mobile payment transactions. The four main banking regulations that also apply to mobile payment are Electronic Funds Transfer Act (EFTA) [3], Truth in Lending Act (TILA) [4], Gramm-Leach-Bliley Act (GLBA) [6], and Payment Card Industry Data Security Standards (PCI-DSS) [5]. These financial regulations are available as large textual documents and require significant human effort to comprehend and parse. Thus, it is difficult to identify which specific rules spread across various banking regulations apply to a mobile wallet transaction in real-time.

We have developed a novel, semantically rich policy-based framework to automate the data security and privacy compliance rules that apply to mobile payments. We have created an integrated knowledge representation of the four main banking regulations that apply to mobile payment, viz. PCI-DSS, EFTA, TILA, and GLBA. This knowledge graph includes compliance rules listed in these regulations for consumers and providers that were automatically extracted using deontic expressions like permission and obligation. Our framework allows complex semantic reasoning that allows consumers to query rules across the four regulations easily. We have validated our design by applying it to six major mobile payment vendors mobile payment policies, including Google Pay, Samsung Pay, Apple Pay, Venmo, Square Cash, and PayPal [26] [27] [28] [29] [30] [31].

In this paper, we present our framework in detail, along with the qualitative and quantitative measures that were used to validate the design against the policies of six major vendors that deal with mobile payments. We have included use cases from both the consumer and provider perspective in this paper. In section II, we discuss related work on PCI-DSS. In section III, we describe various mobile wallet regulations. In section IV, we discuss the architecture flow and the knowledge graph developed by us. Also, the results and discussion are explained in this section. In the last section, we will be concluding with the outcomes.

II. Related Work

A. PCI-DSS

In our previous paper, we have described the PCI DSS ontology developed by us based on the 12 requirements defined by the PCI DSS council [7]. The PCI DSS's goal is to protect cardholder data wherever it is processed, stored, or transmitted. The security controls and processes required

by PCI DSS are vital for protecting cardholder account data, including the PAN – the primary account number printed on the front of a payment card. This includes sensitive data that is printed on a card or stored on a card's magnetic stripe or chip and personal identification numbers entered by the cardholder [7].

If an organization deals with card transactions, it must follow the key policies listed in the sections below. These policies are part of the PCI DSS Version 3.2 [5].

1) Build and maintain a Secure Network: The network configuration and its security requirements should be shared by the IT team and cloud service providers. 'Define a system password and its security parameter' [7]. This means that all the default passwords supplied by the providers should be changed when a system is getting installed in the configured network [7].

2) Protect Cardholder Data: This means that only the necessary data should be stored and at least every quarter, any unnecessary data should be purged. PAN details should be masked, the first six and last four digits are the maximum number of digits you may display. Also, PAN details must be made unreadable wherever it is being stored. 'Encrypt transmission of cardholder data across open, public networks' [7]. This rule of PCI DSS policy asks the organization to use strong cryptography and encryption technologies like SL/TLS, SSH or IPSec, etc. to safeguard sensitive cardholder data during transmission over any networks [7].

3) Maintain a Vulnerability Management Program: All the systems and servers should have anti-virus software to prevent malicious activity. At the same time, anti-virus services should be running in the background and generating auditing logs. 'Develop and maintain secure systems and applications' [7]. This policy ensures that all the patches must be installed on time whenever the vendors publish any new patches. Any changes to the system components, coding of applications must be done through proper change and control procedures. Also, firewall protection should be ensured for any public-facing web applications.

4) Implement Strong Access Control Measures: This policy ensures that access is limited to system components and card holder's data. Also, an access control protocol for systems components should be in place for multiple users, and it must restrict access based on a user's needs and should be set to "deny all" unless correctly authorized. 'Assign a unique ID to each person with computer access'. These policies ensure that any person who is accessing the data should have a unique ID. This will help in tracing an individual's activity in case of any violation or misuse . Also, there should be two-factor authentication for remotely logging into the network, such as making use of RSA token or other technologies that facilitate two-factor authentication 'Restrict physical access to cardholder data' [7]. This ensures that proper facility controls should be applied to the cardholder data environment and individuals only with proper authorization should be allowed to access card holder's data. For visitors, the proper token should be given with an expiry, and a visitor log must be maintained for tracking purposes.

5) Regularly Monitor and Test Networks: This ensures that a secure process should be implemented to link access of individuals to system components. Log activities of the system components must be reviewed daily, and audit trail history must be retained for at least one year so that three months of activity is available immediately. 'Regularly test security systems and processes' [7]. This ensures that all the test procedures should be in place to detect access points and unauthorized users . Also, external and internal penetration testing should be performed, including network and application-layer penetration tests at least annually.

6) Maintain an Information Security Policy: This ensures that the PCI DSS policies that have been established, published, maintained have descriptive, clear definitions of the procedures that everyone in the system knows thoroughly, and such policy must be reviewed at least once a year [7].

III. Regulations that affect Mobile Wallets

We identified that most of the prior research on mobile wallets focuses on the loopholes and provides a detailed explanation of banking regulations. This may not help the consumers or providers since they are usually looking for a source where they can get a list of existing regulations and determine if their organization is complying with them. We focused on this aspect to develop our ontology and and determined that the key regulations, described below, that mobile wallet companies must follow.

A. Electronic Fund Transfer Act/Regulation:

The Electronic Funds Transfer Act (EFTA) was passed in 1978 and codified into law through the FED's Regulation E [14]. The EFTA contains rules and policies for electronic fund transfers (EFT), including any transaction initiated through a computer, telephone, magnetic tape, or electronic terminal. These types of transactions can be initiated through automated teller machines (ATMs), debit card transactions, and direct deposits and withdrawals from a bank account. The regulation generally applies to any financial institutions, but certain provisions apply to any person or any provider dealing in mobile wallets applications or mobile payments. The law applies to mobile wallets too when the underlying payment is made from a consumer's account via an EFT. EFTA is mainly for regulations in the banking sector when there is a payment involving a debit card. Now that in mobile wallets, payment can also be made through a debit card; hence, the EFTA act applies to mobile wallets too. Some of the key obligations for this act is that the rule establishes the consumer rights to several disclosures and error resolution procedures for unauthorized or otherwise erroneous transactions [15]. The disclosures include upfront disclosures regarding, among other things, the terms and conditions of the EFT service and how error resolution procedures will work.

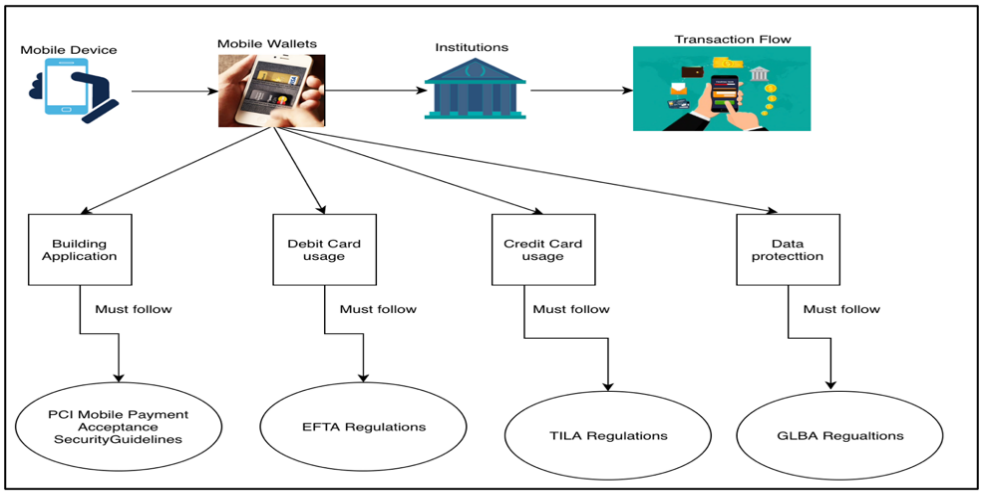

Fig. 1. Overall Architecture Flow

B. Truth in Billing / Regulation:

The Truth in Lending Act (TILA) is part of regulation z, which was codified under FED Regulation Z that establishes the rules surrounding consumer credit [14]. TILA act was formed to give consumers a better sense of the available credit options and better understand various credit line costs. TILA is meant to apply to creditors that offer credit products such as credit cards but may apply to mobile payment systems when mobile payment is funded by a credit card or other TILA covered credit account. It applies to mobile wallets compliance policy when the underlying payment source is a credit card (or other credit account covered by TILA and Regulation Z) [15]. Some of the key obligations that are part of the TILA act are that the Creditors or any organizations are required to provide disclosures to consumers describing costs, including interest rate, billing rights, and dispute procedures. Like EFTA deals in Debit card usage similarly, the TILA act deals in policies regulated for credit card usage.

C. Gramm-Leach-Bliley Act (GLBA) Privacy and Data Security Provisions:

Gramm Leach Bliley Act was enacted in 1999 and was set up for data security guidelines and privacy rules for depository institutions and any non-bank engaged in financial activity [6]. The GLBA applies to any financial institution or non-bank involved in financial activity that handles the personal information of a customer registered for the service; in this case, it is mobile wallets providers. Data security provisions in the GLBA act sets up guidelines for necessary safeguarding of customer nonpublic information that includes customer addresses, phone numbers, bank account numbers, social security numbers, income, and credit histories [6]. The law has been made to protect customer's Personal Identifiable Information (PII). Some of the key obligations that the GLBA act provides are that the institutions are required to provide consumers with the notices regarding the privacy of nonpublic personal information and allow them to opt-out of certain types of information sharing. The GLBA data security provisions give guidance on the appropriate safeguarding of customer information [6]. Thus, this act establishes the rules for consumer privacy and customer data security.

D. PCI Mobile Payment Acceptance Security Guidelines for Developers:

The Payment Card Industry Security Standards Council (PCI SSC) recognizes that merchants may use consumer electronic hand-held devices like smartphones, tablets, wearables or collectively, "mobile devices" that are not solely dedicated to payment acceptance for transaction processing. The PCI mobile payment guidelines contain three objectives for securing mobile payment transactions [5]:

"Objective 1: Prevent account data from being intercepted when entered into a mobile device. If point-to-point encryption (P2PE) is not being used, developers must ensure that a secure transmission path exists between the device used to swipe or input card data and the mobile device".

"Objective 2: Prevent account data from compromise while processed or stored within the mobile device. Any account data stored temporarily on the device must be protected within a secure storage environment. Data retained on the device after transaction authorization must be protected with hashing, truncation, or encryption combined with acceptable key management practices".

"Objective 3: Prevent account data from interception upon transmission out of the mobile device. When cardholder data is transmitted from the device to the next step in the authorization process, it must be protected with strong encryption, such as that provided by Secure Sockets Layer (SSL)/Transport Layer Security (TLS)".

IV. Methodology

In this section, we describe the detailed methodology we used to build and validate our mobile wallets transaction compliance knowledge graph or ontology. We aim to present

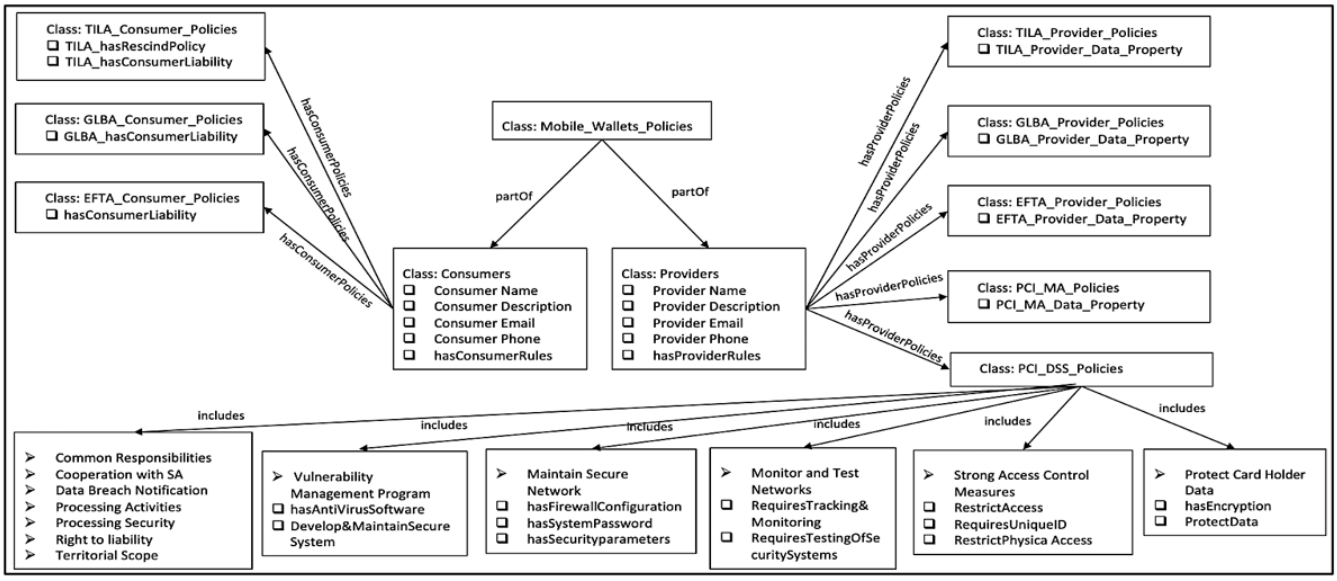

Fig. 2. Integrated Ontology/Knowledgegraph that captures knowledge in TILA, EFTA,GLBA and PCI DSS Regulations

a rich policy-based knowledge representation of the banking regulations that applies to mobile payments. Our methodology is divided into different phases illustrated in Fig. 1. The four stages of our methodology are:

1) Data Collection: Performed extensive research in identifying the regulations that may apply to mobile wallet compliance.

2) Data Pre-processing: For all the four policy regulations, we extracted the relevant rules and key terms from the repository.

3) Ontology Development: Created an Ontology by combining all the four regulations. Detailed information can be found in section C.

4) Evaluation and Validation: The validation of building the knowledge graph was done using publicly available organization policies dealing in mobile wallets.

A. Data Collection

This was the very first process in the methodology. We wanted to know how the mobile wallets process works and how the system is designed in the initial stage. As we mentioned before, there are no compliance policies that are specific to mobile wallets. Policies that apply to banking transactions also apply to mobile payment transactions. Hence, we extensively studied the banking regulations and focused on the mobile wallet specific policies. We reviewed regulations that applied to debit cards and credit cards, the protection of Personal Identifiable Information (PII) of customers stored by financial institutions, and the policy to build an application that deals in mobile payments.

Based on this context for our study, we found the regulation Electronic Fund Transfer Act (EFTA), which is related to debit cards and gift cards. Similarly, we found regulation Truth in Billing Act (TILA), which is related to the usage of credit cards and the Gramm-Leach-Bliley Act (GLBA), which is related to the protection of Personal Identifiable Information (PII) of customers stored by financial institutions. We collected the EFTA, GLBA, and TILA regulations in XML format from the US Government's Code of Federal Regulations (CFR) repository. We also included in this dataset, the policy document PCI Mobile Payment Acceptance Security Guidelines for Developers that is related to building an application dealing in mobile payments. Fig. 1 represents the overall business architecture model for our study.

B. Data Prepossessing

In one of our previous work, we have developed a knowledge graph for the PCI DSS regulation based on the 12 requirements defined by the PCI DSS council [7] [16]. The PCI DSS's goal is to protect cardholder data wherever it is processed, stored, or transmitted. The security controls and processes required by PCI DSS are essential for protecting cardholder account data, including the PAN – the Primary Account Number printed on the front of a transaction card. This includes sensitive data that is printed on a card or stored on a card's magnetic stripe or chip and personal identification numbers entered by the cardholder. In general, if an organization deals in card transactions, then it must adhere to the key policies listed in the PCI DSS checklist [7] [16].

The very first step in our pre-processing process was to integrate the PCI DSS ontology with this study. This is because the mobile payments are part of transaction flow that happens after the setup of mobile wallets, and after the end-user has initiated a payment using mobile wallets. Once the payment is initiated, then organizations must adhere to PCI DSS guidelines [16]. In the next stage, we extracted the repository of EFTA Act [3], TILA Act [4], GLBA Act [6], and PCI MA Policies [5]. In our previous work [7], we were able to

extract relevant key terms from the 12 PCI DSS documents and build knowledge graph accordingly. Similarly, we extracted relevant sections and terms from all the banking regulations to build semantic rich knowledge graph.

After collecting the XML files repository of the four regulations, we converted these documents into text format to extract the key knowledge elements for our knowledge graph. To perform this XML parsing into text, we used the Element Tree Python library [17]. The title of the section was present in the `<subject>` tag, section number of the document was present in the `<sectno>` tag, and the textual contents of the documents in the XML files were present in the `<p>` tag. All three tags are part of `<section>` tag, and we parsed it to extract the contents of the title, section number and verb text and stored them in three different python lists. The next step in the pre-processing stage was to determine key terms and Deontic expressions from the three lists. These two processes are explained in detail below:

1) Key Term Extraction: In our previous work [7], we extracted the key terms of PCI DSS regulation that that are relevant for compliance. Similarly, we identified the relevant key terms for all the four regulations. We used Term Frequency, and Inverse Document Frequency (TF-IDF) [18] to determine the relevant entities from these regulations. This helped us in identifying the instances for our ontology.

2) Deontic Expressions: Modal logic is considered as a broad term that is used to cover various other forms of logic, such as temporal logic and deontic logic [8] [19] [15]. Deontic logic further consists of four types of modalities that helps in classifying statement rules as Permissions, Obligations, Dispensations, or Prohibitions.

- **Permissions / Rights:** Expressions or rules that describe the rights or authorizations for an entity.
- **Obligations:** Expressions that describe necessary actions that an entity must accomplish.
- **Dispensations:** Describe optional expressions and describe non-mandatory conditions.
- **Prohibitions:** Expressions that specify the actions which are not allowed.

To classify Mobile wallets regulation policies in terms of Permissions and Obligations, we extracted sentences containing specific modal keywords like 'will', 'should', 'can', 'could', 'shall', 'must'. These modal verbs enabled us to classify the rule in a sentence into one of the four categories of Deontic logic. This method was vital in answering questions like "When should consumer notify the provider in case of fraud or loss of device". For this study, we have classified the rules into consumer and provider specific Permissions and Obligations. In our previous work, we used text extraction techniques to extract Deontic rules from cloud legal documents [9], PCI DSS regulations [7], and GDPR regulation [8] [10] [15] [17]. We used a similar approach to extract and classify regulation rules into Permissions and Obligations. We used the NLTK library [20] in Python, which helped in Part of Speech (POS) tagging of each sentence in all four documents. Next we formulated grammatical rules based on the POS tags

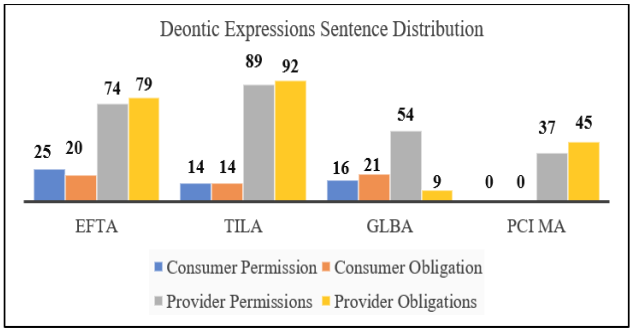

Fig. 3. Deontic Expressions Sentence Distribution

to identify rules in the form of permissions and obligation. Fig. 3 illustrates the deontic sentences distribution for all the regulation documents. The following are examples of some rules we extracted:

Permission

"The amount of any late payment fee and any increased periodic rate(s) (expressed as an annual percentage rate(s)) that may be imposed on the account as a result of late payment. If a range of late payment fees may be assessed, the card issuer may state the range of fees, or the highest fee and indicate that the fee imposed could be lower. If the rate may be increased for more than one feature or balance, the card issuer may state the range of rates or the highest rate that could apply and at the issuer's option an indication that the rate imposed could be lower." [4].

Obligation

"Timely notice is given. Suppose the consumer notifies the financial institution within two business days after learning of the access device's loss or theft. In that case, the consumer's liability shall not exceed the lesser of 50 dollars or the number of unauthorized transfers that occur before notice to the financial institution." [3]

C. Ontology Development and Population

An ontology or knowledge graph can be defined as a shared vocabulary that will help share information of a domain. To be more specific, an Ontology model is said to be the classification of entities that models the relationship between the defined entities. For our framework, we have used OWL [12] and RDF [11] languages to capture the rules defined by the regulations used for this study. These are open source languages developed by WWW Consortium (W3C) and so our ontology, which is in public domain, can be quickly adopted by organizations dealing in mobile payments. It is also platform-independent and so can be easily integrated with PCI DSS [5] and many other data regulation entities. RDF is a language that helps encode knowledge on web space to make the information understandable to electronic agents searching for domain-related information. In this knowledge graph of mobile wallets compliance policies, we have also incorporated our previously built PCI DSS Ontology [7]. We used the Protege [21] software to build and reason over the

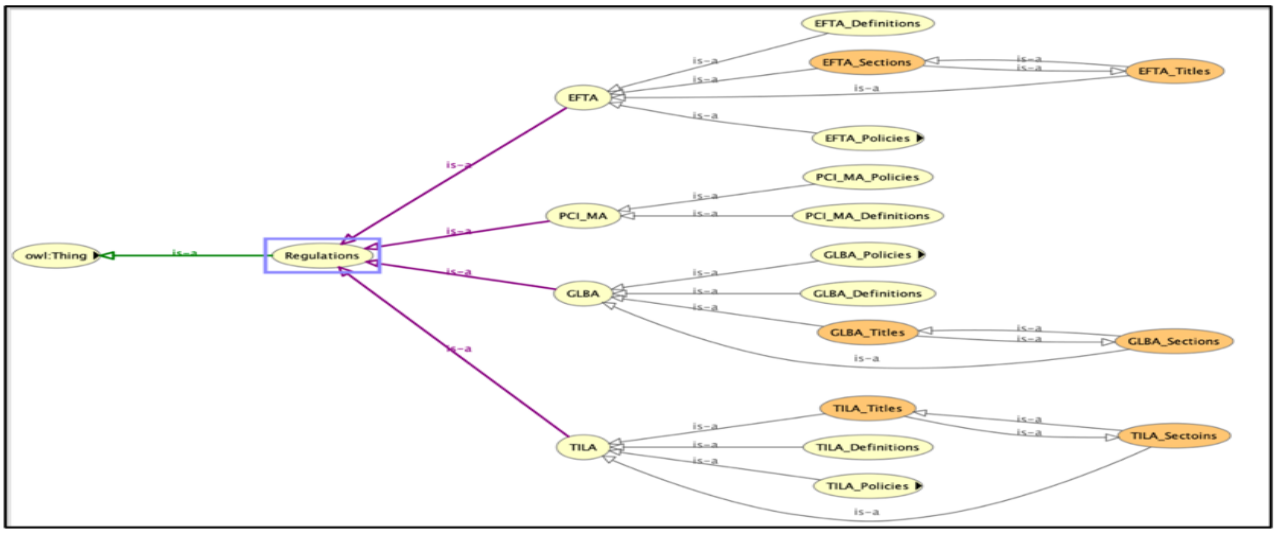

Fig. 4. High Level View of the Regulation Class

knowledgegraph. We have seven main classes along with the imported PCI DSS Ontology [7] as illustrated in Fig. 2. These seven classes are:

- **Consumers:** This class captures the policy rules in all four regulations that apply to consumers of a Mobile Wallets service.
- **Providers:** The class contains the policy rules in all four regulations that apply to mobile wallet service providers.
- **Regulations:** The Regulations class identify the key properties of every regulation. The regulation class has four sub classes “EFTA”, “GLBA”, “TILA” and “PCI MA”. Each of these classes has further sub-classes containing instances of the policy rules and key term definitions. The Regulation class hierarchy is illustrated in Fig. 4.
- **Consumer_Obligations:** This class contains all the rules extracted that are obligated for consumers.
- **Consumer_Permissions:** This class contains all the allowed rules for the consumers.
- **Provider_Obligations:** This class contains all the rules extracted that are obligated for providers.
- **Provider_Permissions:** This class contains all the allowed rules for the providers..

After creating the Ontology, we populated all the classes of the ontology with the key terms and Deontic rules of permission and obligation extracted in the data pre-processing stage. We next reasoned over this integrated knowledgegraph using the SWRL and SPARQL query languages as described below.

1) Semantic Web Rule Language (SWRL): SWRL [22] is a Semantic Web language that is used to express rules as well as logic, combining OWL DL or OWL Lite with a subset of the Rule Markup Language [8]. ”Rules are of the form of implication between an antecedent (body) and consequent (head). The intended meaning can be read as: ”whenever the conditions specified in the antecedent hold, then the conditions specified in the consequent must also hold” [8]. We used SWRL to reason over our Mobile Wallets knowledge graph and query policy specific data. Some of the rules we created are listed in Fig. 5. Using SWRL rules helped us link the EFTA Section class and EFTA Title class. Section 205.1 of EFTA Regulation [3] is named as title ”Authority and Purpose”. SWRL reasoner helped in identifying the instance Authority and Purpose with object property has_EFTASectionNumber as part of Instance, Sec 205.1. Similarly, SWRL reasoning played a significant role in inferencing all the consumer and provider property instances to the instance Consumer_Rules and Provider Rules. As mentioned above, Consumer_Rules and Provider rules are Class Consumer and Provider instances, which contain all the Consumer policies and provider polices applicable for Mobile Wallets Transaction Compliance.

2) SPARQL Query: SPARQL stands for SPARQL Protocol [23] and RDF Query Language and is an RDF query language that is, a semantic query language for the database that helps to retrieve and manipulate data stored in RDF format [11] [13]. With the help of SPARQL Query, we could retrieve policy rules spread across different regulations. We also used Apache Jena Fuseki server and Protege’s SPARQL API to display the results. The SPARQL queries and their output of Consumer liabilities and Provider error resolution from the TILA regulation is illustrated in Fig. 6 and Fig. 7 respectively.

D. Results

1) Evaluation of Knowledgegraph: The evaluation was done using both qualitative and quantitative measures. To evaluate the quality of our knowledgegraph, evaluators used the following metrics as described in [25] on a scale of 5, with 5 being the highest value. The benchmark for each test was 3. The average value for each of the metrics listed below was rated as 4.5 by the evaluators.

SWRL Rules	Description
mw:EFTA_Sections(?S) ^ mw:partof_EFTATitle(?S, ?T) -> mw:has_EFTASectionNumber(?T, ?S)	To infer EFTA Section number for EFTA Titles
mw:Consumers(?S) ^ mw:TILA_Consumer_Policies(?T) ^ mw:TILA_hasConsumerLiability(?T, ?Z) -> mw:hasConsumerRules(?S, ?Z)	To get the Data Property under Consumer class from TILA_Consumer class
mw:Providers(?T) ^ mw:partofProvider_Policy(?S, ?T) ^ mw:TILA_Provider_Policies(?S) -> mw:hasProviderPolicies(?T, ?S)	To get all the individuals under Provider class from TILA_Provider class
mw:GLBA_Consumer_Policies(?S) ^ mw:Consumers(?T) ^ mw:partof_ConsumerPolicy(?S, ?T) -> mw:hasConsumerPolicies(?T, ?S)	To get all the individuals under Consumer class from GLBA_Consumer class
mw:TILA_Consumer_Policies(?S) ^ mw:Consumers(?T) ^ mw:partof_ConsumerPolicy(?S, ?T) -> mw:hasConsumerPolicies(?T, ?S)	To get all the individuals under Consumer class from TILA_Consumer class
mw:partof_GLBATitle(?S, ?T) ^ mw:GLBA_Titles(?T) ^ mw:GLBA_Sections(?S) -> mw:has_GLBASectionNumber(?T, ?S)	To fetch GLBA Title's Section Number
mw:EFTA_Policies(?S) ^ mw:partof_EFTA(?T, ?S) ^ mw:EFTA_Sections(?T) -> mw:has_EFTASectionNumber(?S, ?T)	To infer EFTA Section number and link EFTA instances to EFTA Titles
mw:EFTA_Policies(?S) ^ mw:partof_EFTA(?T, ?S) ^ mw:EFTA_Titles(?T) -> mw:partof_EFTATitle(?S, ?T)	To infer EFTA Section number and link EFTA instances to EFTA Titles
mw:Providers(?S) ^ mw:TILA_Provider_Policies(?T) ^ mw:TILA_Providers_Data_Property(?T, ?Z) -> mw:hasProviderRules(?S, ?Z)	To get all the Data Property under Provider class from TILA_Provider class
mw:Providers(?S) ^ mw:GLBA_Provider_Policies(?T) ^ mw:GLBA_Providers_Data_Property(?T, ?Z) -> mw:hasProviderRules(?S, ?Z)	To get all the Data Property under Provider class from GLBA_Provider class
mw:Providers(?S) ^ mw:PCI_MA_Policies(?T) ^ mw:PCI_MA_Property(?T, ?Z) -> mw:hasProviderRules(?S, ?Z)	To get all the Data Property under Provider class from PCI_MA class
mw:Providers(?T) ^ mw:partofProvider_Policy(?S, ?T) ^ mw:EFTA_Provider_Policies(?S) -> mw:hasProviderPolicies(?T, ?S)	To get all the individuals under Provider class from EFTA_Provider class
mw:Providers(?T) ^ mw:GLBA_Provider_Policies(?S) ^ mw:partofProvider_Policy(?S, ?T) -> mw:hasProviderPolicies(?T, ?S)	To get all the individual under Provider class from GLBA_Provider class
mw:EFTA_Consumer_Policies(?S) ^ mw:Consumers(?T) ^ mw:partof_ConsumerPolicy(?S, ?T) -> mw:hasConsumerPolicies(?T, ?S)	To get all the individuals under Consumer class from EFTA_Consumer class
mw:Consumers(?S) ^ mw:EFTA_Consumer_Policies(?T) ^ mw:hasConsumerLiability(?T, ?Z) -> mw:hasConsumerRules(?S, ?Z)	To get all the Data Property under Consumer class from EFTA_Consumer class
mw:Consumers(?S) ^ mw:GLBA_Consumer_Policies(?T) ^ mw:GLBA_hasConsumerLiability(?T, ?Z) -> mw:hasConsumerRules(?S, ?Z)	To get the Data Property under Consumer class from GLBA_Consumer class
mw:Consumers(?S) ^ mw:TILA_Consumer_Policies(?T) ^ mw:TILA_hasRescindPolicy(?T, ?Z) -> mw:hasConsumerRules(?S, ?Z)	To get the Data Property under Consumer class from TILA_Consumer class

Fig. 5. SWRL Rules we created to reason over the knowledgegraph to query rules spread across various Mobile Wallet regulations

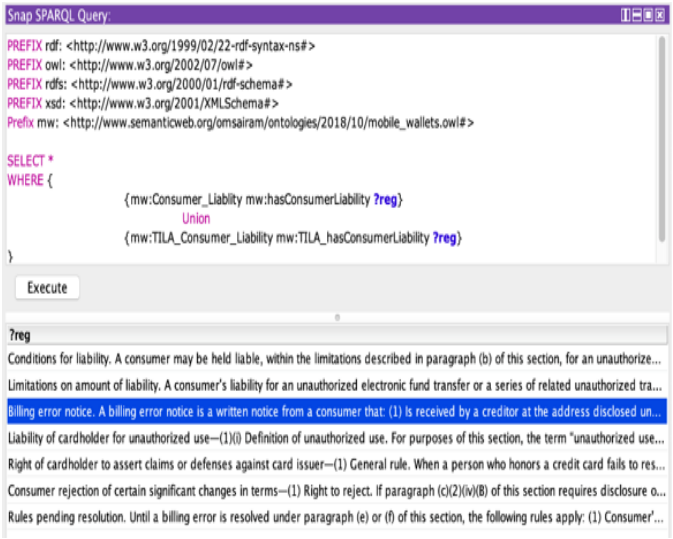

Fig. 6. SPARQL Query - Consumer's Liability rules from TILA

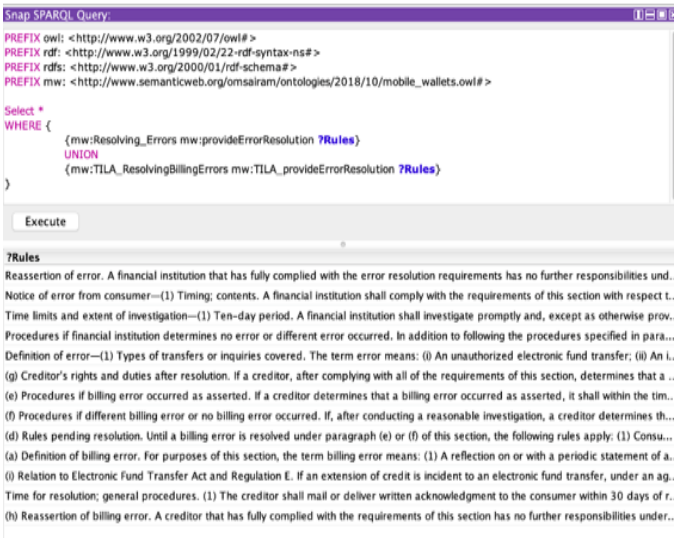

Fig. 7. SPARQL Query - Provider's Error Resolution rules in TILA

Accuracy determines if the definitions, descriptions of classes, properties, and individuals in an ontology are correct.

Completeness measures if the domain of interest is appropriately covered in this ontology.

Conciseness determines if the ontology includes irrelevant elements with regards to the domain to be covered.

Adaptability measures how far the ontology anticipates its uses. An ontology should offer the conceptual foundation for a range of anticipated tasks.

Clarity measures how effectively the ontology communicates the intended meaning of the defined terms. Definitions should be objective and independent of the context.

Computational efficiency measures the ability of the used tools to work with the ontology, the speed that reasoners need to fulfill the required tasks.

Consistency describes that the ontology does not include or allow for any contradictions.

To determine our accuracy rate, we measured how many keyterms were classified correctly by our system by considering precision and recall. We checked for average accuracy in finding the average per key term effectiveness of a classifier. Results obtained for the accuracy, precision and recall were 64.95%, 55.2% and 92.5%. We are currently working on improving the accuracy of how the rules are classified.

2) Validation with Leading Providers: For the validation process, we referenced the policies of major mobile wallet service providers in the market with massive transaction volume like Google Pay [26], Samsung Pay [27], Apple Pay [28], Venmo [29], Square Cash [30], and PayPal [31]. We searched for the key terms in their policies, like Consumer, Error, Privacy, Disclosures, protections, statements, fraud, loss, and liability. Fig. 8 shows the policies that were used to validate our approach and the frequency of these key terms in all the policies. We have utilized these key terms to populate

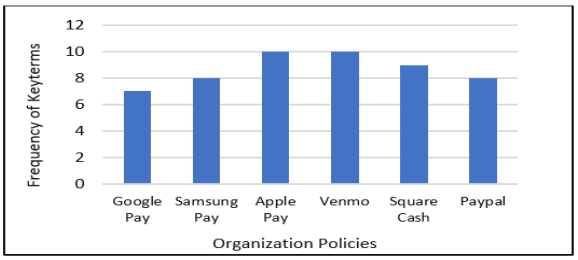

Fig. 8. Validation Results

the instances of respective classes in ontology.

V. Conclusion

We have developed a semantically rich knowledgegraph to represent mobile wallet policies by integrating knowledge from various banking and credit card regulations like PCI-DSS, EFTA, TILA, and GLBA. As these regulations are in textual format, it is difficult for organizations to comply in real time with the rules described in these vast documents. For converting these textual documents into a graph-based ontology, we first identified the most common terms or key terms and extracted them from all four regulations. We used TFIDF technique to determine the documents' relevant entities. This technique also helped us map and populate our ontology instances with the key terms occurring in multiple regulatory policies. Using Deontic Logic with text extraction approaches, we extracting the permissions and obligation rules in all four documents and classified them under consumer and provider rules.

This knowledge graph, available in the public domain, can be used to reason over and notify consumers or providers, at near real time, if there is any violation of a mobile wallet policy. One interesting observation is that most of the key terms are found across all the mobile wallet regulations that we included in this study.

Our ontology is semi-automated based on the key terms extracted from various financial regulations in this study. For future work, we want to automate and populate in our ontology completely. We are also developing an easy-to-use graphical interface that will enable end-users to query and reason over this knowledge graph and take quick actions.

Acknowledgment

This work was supported in part by a DoD Supplement to NSF award 1747724, Phase I IUCRC UMBC: Center for Accelerated Real time Analytics (CARTA).

References

[1] Adam J. Levitin Pandora's Digital Box: The Promise and Perils of Digital Wallets, 166 U. Pa. L. Rev. 305 (2018).
[2] P. M. E. Budnitz, "The Legal Framework of Mobile Payments" 2016. https://www.pewtrusts.org/-/media/assets/2016/02/legal_framework_of_mobile_payments_white_paper.pdf
[3] C. O. F. Regulations, "Electronic Fund Transfer Act/ Regulation E" [Online]. Available: https://www.govinfo.gov/content/pkg/CFR-2012-title12-vol2/xml/CFR-2012-title12-vol2-part205.xml.
[4] C. O. F. Regulations,"Truth in Lending Act/ Regulation Z," [Online]. Available: https://www.govinfo.gov/content/pkg/CFR-2012-title12-vol8/xml/CFR-2012-title12-vol8-part1026.xml.
[5] P. S. S. C. Emerging Technologies, "PCI Mobile Payment Acceptance Security Guidelines," September 2017. [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_Mobil_Payment_Acceptance_Security_Guidelines_for_Developers_v2_0.pdf.
[6] C. O. F. Regulations, "GRAMM-LEACH-BLILEY ACT," [Online]. Available:https://www.govinfo.gov/content/pkg/CFR-2014-title17-vol2/xml/CFR-2014-title17-vol2-part160.xml.
[7] Nagar, A., Joshi, K. P. (2018, May). A semantically rich knowledge representation of PCI DSS for cloud services. In 6th International IBM Cloud Academy Conference ICACON 2018, Japan.
[8] Elluri, L., Nagar, A., Joshi, K. P. (2018, December). An integrated knowledge graph to automate gdpr and pci dss compliance. In 2018 IEEE International Conference on Big Data (Big Data) (pp. 1266-1271).
[9] Joshi, Karuna Pande, and Claudia Pearce. "Automating cloud service level agreements using semantic technologies." 2015 IEEE International Conference on Cloud Engineering.
[10] Joshi, K. P., Elluri, L., Nagar, A. (2020). An Integrated Knowledge Graph to Automate Cloud Data Compliance. IEEE Access, 8, 148541-148555.
[11] O. Lassila, R. Swick and others, Resource Description Framework (RDF) Model and Syntax Specification, WWW Consortium, 1999.
[12] D. McGuinness, F. Van Harmelen, et al., OWL web ontology language overview, W3C recommendation, World Wide Web Consortium, 2004.
[13] Rusu, Delia, et al. "Triplet extraction from sentences." Proceedings of the 10th International Multiconference" Information Society-IS. 2007..
[14] S. Congdon, "WHAT'S IN YOUR WALLET? ADDRESSING THE REGULATORY GREY AREA SURROUNDING MOBILE PAYMENTS".
[15] Elluri, Lavanya, Karuna Pande Joshi, and Anantaa Kotal. "Measuring Semantic Similarity across EU GDPR Regulation and Cloud Privacy Policies." UMBC Student Collection (2020).
[16] P. C. I. S. S. Council, https://www.pcisecuritystandards.org/document_library, April 2016.
[17] L. Elluri and K. P. Joshi, "A Knowledge Representation of Cloud Data Controls for EU GDPR Compliance," 2018 IEEE World Congress on Services (SERVICES), San Francisco, CA, 2018, pp. 45-46, doi: 10.1109/SERVICES.2018.00036.
[18] "TF-IDF," [Online]. Available: https://en.wikipedia.org/wiki/Tf
[19] "Modal Logic," [Online]. Available:http://plato.stanford.edu/entries/logic-modal/.
[20] "NLTK Documentation," [Online]. Available: https://www.nltk.org/.
[21] Musen, M.A. The Protégé project: A look back and a look forward. AI Matters. Association of Computing Machinery Specific Interest Group in Artificial Intelligence, 1(4), June 2015. DOI: 10.1145/2557001.25757003.
[22] Horrocks, I., Patel-Schneider, P. F., Boley, H., Tabet, S., Grosof, B. Dean, M. (2004). SWRL: A Semantic Web Rule Language Combining OWL and RuleML (W3C Member Submission). World Wide Web Consortium .
[23] Wikipedia contributors. (2021, January 20). SPARQL. In Wikipedia, The Free Encyclopedia. Retrieved 22:57, April 4, 2021, from https://en.wikipedia.org/w/index.php?title=SPARQLoldid=1001605350
[24] Kemp, Richard. "Mobile payments: Current and emerging regulatory and contracting issues." Computer Law Security Review 29.2 (2013): 175-179.
[25] Brank, J., Grobelnik, M., Mladenic, D. (2005, October). A survey of ontology evaluation techniques. In Proceedings of the conference on data mining and data warehouses (SiKDD 2005) (pp. 166-170). Citeseer Ljubljana, Slovenia.
[26] "Google Wallet" [Online].Available: https://wallet.google.com/files/error-resolution.html
[27] "Zions Bank" [Online]. Available: https://www.zionsbank.com/pdfs/samsung-pay-terms-of-use.pdf
[28] "Greendot" [Online]. Available: https://applecash.greendot.com/termsconditions/
[29] "Venmo" [Online]. Available: https://venmo.com/legal/us-payment-method-rights
[30] "Cash App" [Online]. Available: https://cash.app/legal/us/en-us/card-agreement
[31] "Paypal" [Online]. Available: https://www.paypal.com/us/webapps/mpp/ppcterms