**INTRODUCTION**

NOWADAYS, to obtain the overall picture of the fast evolving cyber threat situation and protect themselves from the complicated, persistent, organized, and weaponized cyber-attacks, a rising number of organizations across the world are showing an increasing willingness to leverage the open exchange of cyber threat intelligence (CTI) [1]. CTI is evidence based knowledge about an existing or emerging threat to assets and can be used to inform decisions regarding a subject’s response to the threat [2]. As we know, cyber criminals usually make full use of network infrastructures (e.g., domain names and Internet Protocol or IP addresses) to conduct cyber-attacks. The Pyramid of Pain model [3] indicates six levels of threat indicators for detecting attack activities, and the lower three levels are file hashes, IP addresses, and domain names. These three levels are atomic indicators and can be consumed by network security devices such as intrusion detection system (IDS), firewall, and spam filters on email servers. Through theapplication program interfaces (APIs) provided by the threat intelligence sharing platforms (TISPs), users can acquire huge amounts of CTI about file hashes, IP addresses, and domain names (i.e., the lower three levels of the Pyramid of Pain model that are the focus of this study). Generally, diverse intelligence sources can help depict cyber-threat infrastructure nodes from different perspectives. For instance, a domain name can be described with information not only from commercial CTI sources such as IBM X-Force Exchange Platform1 and ThreatBook2 but also from the related datasets such as passive domain name system (DNS) and domain name blacklist. Facing increasingly sophisticated cyber-attacks, modeling CTI provides numerous advantages [4], [5], [6], [7], such as obtaining a full picture of the fast-evolving cyber threat situation and unveiling potential groups that are behind specific attacks. Take domain name infrastructure nodes as an example, the threat types of domain names can be spam URLs, brute force login attacks, malware activity, and bot net node activity. Identifying the threat types of infrastructure nodes not only benefits the fine-grained threat warning but also facilitates targeted defensive measures. Note that we only consider CTI represented in structured data in this research. The extraction of structured data from unstructured data such as security technique reports is another important research direction [8], [9].

**1.1 Motivation**

The modeling of CTI and the threat type identification of infrastructure nodes should undoubtedly be the most fundamental requirements for any cyber threat defense and warning system. In the past few years, academic and industry communities in the fields of cyber security and data mining have been attracted to this topic, and many state-of-the-art studies have been carried out, such as [7], [10] and [11]. Some of them are very creative and elaborate, but most of them face the following two key limitations that must be solved.

First, few studies have focused on the problem of limited threat type labels of infrastructure nodes involved in CTI. Owing to the high cost of manual labeling, the threat labels of cyber threat infrastructure nodes is incomplete in the CTI database, and the labels are annotated with threat types by intelligence providers or security analysts [11]. Thus, how to accurately and effectively learn from the limited labeled infrastructure nodes and a large number of relationships among them to predict the threat types of unlabeled nodes is a paramount concern and key task for most security analysts and operators [11].

Furthermore, few studies have focused on the higher-level semantic relations among cyber-threat infrastructure nodes from the perspective of heterogeneous information network (HIN) [12]. In a large-scale CTI sharing environment, graphbased automatic analysis has attracted significant research efforts in recent years [5], [10], [13]. However, most of these works primarily focus on homogeneous information networks or bipartite graphs, which cannot discover the higher-level semantic relations among different types of nodes. As a special type of information network, HIN involves multiple types of nodes or relations, which have different semantic meanings. Such complex and semantically enriched information networks have great potential for knowledge discovery [14], [15]. However, the application of HIN in CTI mining is largely unexplored. Although some works have considered multiple types of nodes and relations, they have not considered higher-level semantics. Modeling CTI on HIN can provide an efficient and compact representation of linked cyber-threat infrastructure nodes in various semantics, such as capturing the complex relations among different types of infrastructure nodes, distinguishing different cyber-attacks based on the differences of network behaviors, and exploring how adversaries organize campaigns and adapt their techniques. Thus, a practical model for CTI on HIN, which leverages network correlations for better mining of CTI, should be further explored to relieve security analysts from heavy analysis work [16].

**1.2 Our Contributions**

To the best of our knowledge, we are the first to simultaneously design a HIN for CTI modeling, and propose a meta-path and meta-graph instances-based threat infrastructure similarity (MIIS) measure-based heterogeneous graph convolutional network (GCN) approach for threat type identification of cyber-threat infrastructure nodes. The main innovations of our mechanism go beyond those of existing approaches in terms of the following three aspects:

1) A CTI modeling approach based on HIN is proposed from the perspective of computation (meta-path and meta-graph instances based computing). By modeling CTI based on HIN, the proposed framework can not only integrate infrastructure nodes involved in CTI in a semantically meaningful way, including domain name, IP addresses, malware hashes, email addresses, and their relations but also extract and incorporate higher-level semantics of infrastructure nodes.

2) A MIIS measure-based heterogeneous GCN approach is proposed to identify the threat types of infrastructure nodes. We define a MIIS measure between threat infrastructure nodes, and present a MIIS measure-based heterogeneous GCN approach to identify the threat type of infrastructure nodes. Through hierarchical regularization, the approach can alleviate the problem of over fitting and achieve good results in the threat type identification of infrastructure nodes. This research can also promote cyber security investigations with partial or incomplete information.

3) A practical system called Hin CTI is developed for modeling cyber threat intelligence and identifying threat types. With the system, we conduct comprehensive experiments on real world datasets, and experimental results demonstrate that our proposed approach can significantly improve the performance

of threat type identification compared with the existing state-of-the-art baseline methods.

These innovative designs collectively make Hin CTI an efficient solution that can be used in the complex cyber security environment. A series of comprehensive experiments based on the real-world cyber-threat data from IBM X-Force Exchange Platform and other sources are conducted to evaluate the effectiveness and efficiency of the proposed approach. Experimental results demonstrate the superiority of the proposed approach by comparison with the state-of-the-art baseline methods.

The rest of the paper is organized as follows. Section 2 discusses the related work. Section 3 depicts the modeling of CTI on HIN, presents preliminary concepts, and gives an overview of the system architecture. Section 4 gives a detailed description of the proposed heterogeneous GCN-based threat type identification approach. Section 5 describes the experiments and performance results of the proposed approach by comparison with the state-of-the-art baseline methods. Section 6 summarizes the paper and outlines future work.