近些年来，随着信息技术的飞速进步与发展，网络安全技术不断演化，无论是以5G通讯，物联网等新型网络形式的出现，还是以在线社交网络等为代表的新型服务模式的出现，都不断呈现出开放性、异构性、移动性和可信性的特点，这些服务方便了人们的生活，但是由于网络的匿名性，人们同时也遭受着非法网络渗透等带来的巨大损失和伤害。针对日益庞大的网络用户的威胁情报数据，如何对这些威胁情报进行合理的分析和研究将成为新时代下社会信任体系与主动安全防御的重中之重。

现今的互联网环境下，人们对用户实体的威胁情报数据的主要来源就是网络，尤其是大规模的在线社交网络，但是社交网络中的威胁情报数据具有匿名性，同时具有数据规模大，关联关系复杂等特点，如何有效的对这些用户实体的威胁情报数据进行高效并且合理的研究与利用，是解决网络空间环境下，对网络用户的威胁情报进行信任评估的关键。

因此，本文主要针对大规模在线社交网络环境中的威胁情报的信任评估问题进行研究，主要的工作任务如下：

（1）针对大规模在线社交网络环境中，威胁情报数据规模大、关联关系复杂的特点，本文提出了一种基于机器学习方法的海量数据知识图谱构建的方法。该方法利用网络空间中威胁情报数据的结构化和非结构化特性，对原始的威胁情报数据进行实体、属性和关系的抽取；考虑抽取得到的实体、属性和关系信息之间存在重复、别名问题，再利用知识融合的技术对抽取得到的实体、属性和关系进行加工、整合、消除歧义；最后，针对得到的实体别名不一致或者冲突的问题，本文采用二分类的机器学习方法来消除异构实体数据存在的冲突问题。这样，就可以得到一系列基于事实表达的高质量的威胁情报知识图谱，构建的威胁情报知识图谱质量越高，将使得基于知识图谱的信任评估计算越精确。

（2）针对网络环境中用户情报数据的匿名特点，本文提出了一种基于知识图谱的用户情报数据的信任评估模型。该模型首先利用知识表示TransE（Translating Embeddings）算法威胁情报知识图谱中的实体、属性和关系等节点信息映射成低维向量空间的向量；为了计算两个节点之间的信任关系，我们提出一种基于循环神经网络（Recurrent Neural Network, RNN）的路径聚合算法来计算得到两个节点之间任意一条路径的信任数值，然后通过路径可靠性算法（Path Reliability Measuring Algorithm，PRM）对两节点之间存在的多条关系路径进行信任关系的加权计算，实验结果表明，基于上述的威胁情报信任评估模型，相较于传统的基于规则运算的模型，具有较高的准确度。

（3）针对现实网络环境中的用户信任评估的需求，本文基于新浪微博，设计并且实现了一套新浪微博用户情报数据的可信评估系统。该系统分为威胁情报数据爬取模块、威胁情报数据预处理模块、威胁情报知识图谱构建模块、威胁情报可信分析模块。其中情报数据爬取模块利用网络爬虫对新浪微博的用户情报数据进行爬取；威胁情报数据预处理模块旨在对原始的结构化威胁情报数据进行实体、属性和关系的解析；威胁情报知识图谱构建模块利用获取到的威胁情报数据，利用知识图谱的构建方法，构建高质量的威胁情报知识图谱；威胁情报信任分析模块将利用上述路径聚合算法和路径可靠性算法对威胁情报进行信任关系的可信评估；最后，系统额外提供可视化平台用户对构建的知识图谱进行可视化展示。