PROJECT SUMMARY

Overview:

Massive knowledge graphs are powering today's intelligent applications in many sectors. However, many knowledge graphs are proprietary, and are only available to users through a limited query interface (if available at all). The lack of open access to large-scale, real knowledge and data bases hurts transparency and social equity, and hampers scientific progress. There is thus a pressing need for an open knowledge network---a shared knowledge infrastructure of public, semantically interlinked, community-driven data equipped with adequate tools for exploitation. The goal of this project is to develop new capability and resources for enabling a credible open knowledge network that can help ensure the quality of knowledge-rich applications and aid in debunking misinformation. The notion of data credibility is utmost important, as human societies today are struggling with an unprecedented amount of falsehoods which harms wealth, democracy, health, and security. Yet, credibility has been much less studied by research on knowledge graphs, and is often considered as an afterthought. Toward this goal, a multidisciplinary project team will conduct use-inspired, convergence research on the following cross-cutting horizontal research areas: (1) Modeling credible knowledge graphs, deciding what types of knowledge need to be captured in order to promote credibility, and how such knowledge should be represented in order to enable computational approaches. (2) Developing data-driven understanding of what factors contribute to the persuasiveness of factual statements, what signals help gauge credibility, and how to exploit them to design effective countermeasures against misinformation. (3) Designing and implementing computational methods that leverage knowledge graphs to vet factual statements and generate convincing explanations of the verdicts. (4) Devising procedures and mechanisms for bootstrapping a credible open knowledge graph and for maintaining and growing it over time in a way that ensure credibility. While researching in these horizontal areas, the project will focus on several vertical application domains with timely practical relevance, including combating falsehood in media, debunking health-related misinformation, and mitigating security threats from software vulnerabilities and illicit markets.

Keywords: knowledge graphs; credibility; open access; fact-checking; health misinformation; security

Intellectual Merit:

This project addresses a highly important need that has not received much attention till this date---the need for fundamentally enabling credible knowledge graph and using it to aid misinformation debunking. For enabling an open knowledge network, while many may focus on classic research questions related to semantic web, querying and user interface, security and privacy, and data integration, this project tackles the novel aspect of credibility, which shall become another pillar in this area of research and complement other endeavors. This project is driven by a research agenda that thoroughly synthesizes principles and methods from multiple distinctive disciplines. The findings of this transformative research will radically change understanding of (mis)information consumption and mitigation, and will trigger a new line of investigation.

Broader Impacts:

In developing an open knowledge network, it is imperative to ensure credibility---truthfulness, integrity and completeness, since data quality directly impacts the utility of data-driven insights and decisions. A credible open knowledge network will empower several areas of national importance. First, it will become an indispensable data source for debunking misinformation, which is vital to a society struggling with an unprecedented amount of falsehood. Second, it helps secure the cyberspace and protect both digital and real worlds. Third, it can help improve the human condition by transforming healthcare with intelligent computing that promotes and supports health-related decisions using reliable data. Therefore, the project has potential societal, economic, and educational impact on a broad range of individuals, governments, corporates, and nonprofits. The project will also provide training to a large number of students, which will aid the development of a diverse and globally competitive workforce.

RAISE: C-Accel Pilot - Track A1: Credible Open Knowledge Network

PI: Chengkai Li, The University of Texas at Arlington

1 Results from Prior NSF Support

PI Chengkai Li and **Co-PI Jun Yang**, during their ten-year collaboration, have been awarded two joint NSF grants, both closely related to this project. The more recent NSF support is "III: Small: Collaborative Research: Towards End-to-End Computer-Assisted Fact-Checking," 9/1/17 - 8/31/20, IIS #1719054 (UTA, PI: Li, Co-PI: Mark Tremayne, who is also on this team) and #1718398 (Duke, PI: Yang), total $500,000. The two PIs' earlier joint NSF grant is "III: Medium: Collaborative Research: From Answering Questions to Questioning Answers (and Questions)—Perturbation Analysis of Database Queries," 09/01/14 - 08/31/19, IIS #1408846 (Duke, PI: Yang), #1408928 (UTA, PI: Li) and #1408915 (Stanford), total $1,200,000. **Intellectual Merit:** Award #1719054 / #1718398 funds a systematic study towards ClaimBuster, an end-to-end system for computer-assisted fact-checking. The project so far has produced significant publications in SIGMOD, VLDB, IJCNN, CIKM, ACL, and other venues [161, 162, 85, 33, 97, 31, 30, 37]. Award #1408846 / #1408928 funds the study of perturbation analysis of database queries, a key technology enabler for computational fact-checking. This project led to numerous publications in prestigious venues (e.g., SIGMOD, PVLDB, ICDE, EDBT, CIKM, TODS, TKDE, KDD, TKDD) [151, 153, 140, 144, 160, 76, 75, 73, 77, 143, 145, 74, 78, 152, 158]. In these projects the PIs developed several publicly available online prototype and demonstration systems such as ClaimBuster (demo at [10] and video at [14]) and iCheck (demos at [153, 144, 143]) for fact-checking, ClaimPortal for monitoring factual claims in social media (demo at [11] and video at [15]), Squash for real-time matching and delivery of fact-checks (demo at [30]), and Maverick and FactWatcher (demo at [18] and video at [16]) for discovering data-backed facts (demo at [18] and video at [16]). The research products have received several awards, including an SIGMOD most reproducible paper award [157], a first runner-up award in the SIGMOD'17 undergraduate student research competition, and a VLDB'14 excellent demonstration award to FactWatcher [76]. **Broader Impacts:** ClaimBuster benefits a large base of potential users including consumers, publishers, corporate competitors, and legal professionals, among others. The ClaimBuster API is being used by the Duke Reporters' Lab to create daily news alerts that recommend the most check-worthy factual claims from CNN programs, social media, and congressional records to The Washington Post, PolitiFact, and other fact-checkers. There is a news report [25] about how ClaimBuster helped The Washington Post fact-check a claim which, as The Post stated, "would have been lost to history if it had not been for ClaimBuster." Among the Ph.D. student contributors to the two prior NSF projects, You Wu graduated from Duke in 2015 and joined Google, working in a group led by Cong Yu (who is a collaborator on this project team) on improve Web credibility; Naeemul Hassan (who is also on this project team) graduated from UTA in 2016 and joined the University of Mississippi as an assistant professor; Gensheng Zhang graduated from UTA in 2017 and joined Google as a software engineer; Afroza Sultana graduated from UTA in 2018 and became a software engineer at Teradata Lab; Brett Walenz graduated from Duke in 2019 and joined Google as a software engineer. Many students with diverse backgrounds have participated in the projects at UTA and Duke, including one Hispanic Ph.D. student who is also a former REU student, five female Ph.D. students, two female M.S. students, one Black M.S. student, and numerous undergraduates including one Hispanic, one African American, and many women.

Co-PI Sibel Adalı has worked on and served in leadership positions on multiple collaborative projects, some of which are funded by different agencies. She has lead research efforts in computation models of trust [32, 50, 125] with its applications to information credibility and news related misinformation (further details on team expertise section). The closest NSF fundings are (EAR-1541017 $29,920, 9/1/2015 - 8/31/2017, and EAR-0949318, $762,000, 9/1/2010 - 8/31/2017) aimed at creation of infrastructure to facilitate sharing of research data and findings in Metamorphic Petrology field of Geology [139, 20]. **Intellectual Merit:** This work created common data models for geologists, research data being made public and an open source software (Metpetdb), presented in multiple AGU meetings. **Broader Impacts:** The system is integrated into the EarthChem system combining geological data from different disciplines.

Co-PI Xiaojing Liao is the PI of the project: "SaTC: CORE: Medium: Collaborative: Understanding and Discovering Illicit Online Business Through Automatic Analysis of Online Text Traces" (CNS-1850725, $1,200,000, 07/20/2018 - 08/31/2020) which focuses on systematically studying how to automatically discover criminals' communication traces and intelligently utilize them to fight against online crime. **Intellectual Merit:** The project has resulted in several high-impact publications at leading venues [146, 159, 101, 89, 62, 48]. **Broader Impacts**: The project contributes to the progress of new interdisciplinary research on applying NLP and learning techniques to support intelligent security protection. The findings were broadly disseminated through various talks, courses taught at IU. With the support of this grant, Dr. Liao is currently supporting two female Ph.D. assistants.

Co-PI Yinghui Wu is the PI of the project: "BIGDATA: Collaborative: F: Association Analysis of Big Graphs:

Models, Algorithms and Applications" (IIS-1633629, $321,678, 09/01/16 - 08/31/19). **Intellectual Merit:** Association analysis is a fundamental problem in Big Data analysis. We proposed a new generation of association discovery framework, including a class of graph association rules and resource-aware mining over heterogeneous graphs. This ongoing project has produced publications in top-tier conferences and journals [108, 107, 106, 110, 61, 60, 137, 93, 132, 111, 51, 124, 156], including an ACM Research Highlight Award, a SIGMOD best paper award [61] and a VLDB best demo award [60]. **Broader Impacts**: The project supported the work of two Ph.D. students and one female master student. It also led to a new undergraduate level course ("Big Data") at WSU.

2 Overview

Massive knowledge graphs are powering today's intelligent applications in many sectors. These graphs record facts—properties of entities (nodes) and relationships (edges) between them. They represent encyclopedia-type information, domain-specific data (e.g., government datasets and biomedical databases) and proprietary data such as social graphs and product-customer databases. However, many knowledge graphs are proprietary. They are only available to users through search or canned queries, or not available at all. Even knowledge graphs in the public domain pose substantial barriers to full exploitation due to their heterogeneity, data quality issues, difficulty in semantic linking and integration, lack of tools for secure and privacy-preserving access, and lack of natural user interfaces for querying and data exploration. The lack of public access to large-scale, real datasets will hurt transparency and social equity and will hamper scientific progress in many areas. There is thus a **pressing need** for an open knowledge network—a shared knowledge infrastructure of public, semantically interlinked, community-driven data equipped with adequate tools for exploitation. This concept is gaining traction, leading to a multitude of efforts in industry, governments and academia at both domestic and international levels [69]. Decades of research and development in areas such as semantic web, data integration and fusion, data cleaning, database query, security and privacy, and human-computer interaction has accumulated vast experience in tackling aforementioned challenges and will continue to be crucial in the endeavor of creating an open knowledge network.

The **goal** of this project is to develop new capability and resources for enabling a *credible* open knowledge network—knowledge graphs with truthful information that ensure the quality of knowledge-rich applications and aid in debunking misinformation. The notion of data credibility is of utmost importance, as our society is struggling with an unprecedented amount of falsehood which harms wealth, democracy, health, and security. Yet, it is under examined compared to with aforementioned areas. Thus, this research will complement advancements in those other domains and together help realize the vision of open knowledge network. Toward this goal, our multidisciplinary team will conduct use-inspired, convergence research on the following **cross-cutting horizontal research areas**.

A) Data modeling for credible knowledge graphs. We will research data modeling challenges and solutions in enabling credibility as a "first-class" property of knowledge graphs. More specifically, we will study how to support assessing the veracity of facts recorded in knowledge graphs under a data model that captures the temporal aspect of evolving data, data lineage and provenance, and source reputability. The data model should accommodate linking factual claims to data, recording conflicting facts, and even allowing the residency of debunked misinformation which would enable techniques that require "negative" examples.

B) Data-driven understanding of persuasiveness of factual claims and effectiveness of intervention mechanisms. To effectively vet factual claims using knowledge graphs, we aim at gaining insights regarding 1) what factors make people accept a (false) claim, 2) what traits of such claims can help assess their veracity, and 3) what intervention mechanisms are effective in countering such false claims. Particularly, with respect to the first question, we will identify what contributes to the persuasive power of factual statements. Regarding the second question, we will investigate challenges in measuring credibility, e.g., what signals are more effective than others in establishing truthfulness? Finally, with regard to the third question, we will study how to better present fact-checking results, specifically how to persuasively explain the verdict on a factual claim from an algorithmic fact-checking tool. The examination of these questions will be guided by cognitive and communication principles. Our focus and approach is data-driven, based on fine-grained analysis of linguistic elements in factual claims and how they connect to knowledge graphs, a salient characteristic distinguishing this study from conventional psychology and communication theories.

C) Vetting factual claims using knowledge graphs. We will invent methods for exploiting the credible open knowledge network in vetting factual claims. This task will be investigated in two complementary directions. 1) We will develop methods for verifying claims through querying databases, particularly by devising algorithms to convert factual claims into queries and use the query results to discern the claims' truthfulness. This will leverage the outcome of our ongoing projects, with the distinctive focus on exploring the idiosyncrasies of knowledge graphs and the vertical application domains of healthcare and security. 2) We will devise methods to automate the generation of explanations of the aforementioned algorithmic vetting process and its results, including the role of knowledge graphs in them. The

implementation of such AI-explainability methods will be grounded in social science theories and our findings from B) regarding the persuasiveness of both claims and explanations of vetting results. This consideration is particularly pertinent to fact-checking, since algorithm-aided tools lacking explanations unlikely will gain people's trust.

D) Improving the credibility of knowledge graphs. For preparing data, we will leverage existing datasets (e.g., Wikidata, Freebase, YAGO, many more in Linked Open Data [19], and datasets from repositories such as usafacts.org and data.gov), either knowledge graphs themselves or converted into knowledge graphs. We will also leverage our existing expertise in crowdsourcing and in constructing knowledge graphs by extraction from textual documents (e.g. Yunyao Li and Marina Danilevsky have built industrial strength knowledge bases at IBM through approaches including text extraction). Our focus in this task, though, is to improve the credibility—a data quality trait—of knowledge graphs by two means. One is to develop erroneous data detection and repairing methods so as to correct untruthful factoids in existing knowledge graphs. Specifically, we will develop outlier detection algorithms for finding potential erroneous facts and data repairing methods for automating the correction of inaccurate facts. Another approach that we will explore is to bootstrap and continuously grow the credible open knowledge network. Particularly, we will develop techniques for inferring new facts from existing facts by rule mining systems and machine learning methods that use latent features, as well as synthesizing information from multiple sources.

While conducting research in these cross-cutting horizontal areas, our focus will be particularly on several **vertical application domains**. Beyond falsehood in news, the research will aid debunking health-related misinformation as well as security threats related to software vulnerabilities and illicit markets. Consider FDA's drug adverse event database which can be converted into a knowledge graph. The proposed research can help debunk false claims that harm public health, such as anti-vaccine misinformation and misbeliefs in self-care chronic conditions. With regard to cybersecurity, adversaries were found to post fake attack indicators for misleading or evading attack detection mechanisms. We aim at constructing and evolving a credible knowledge network for recovering cyber threat attack lifecycle, using which we will innovate techniques to capture attack campaigns, recognize their targets, determine their origins, and pinpoint weak links in attack infrastructures.

Intellectual Merit This project addresses a highly important need that has not received much attention till this date—the need for fundamentally enabling credible knowledge graph and using it to aid misinformation debunking. For enabling an open knowledge network, while many may focus on classic research questions related to semantic web, querying and user interface, security and privacy, and data integration, we tackle the novel aspect of credibility, which shall become another pillar in this area of research and complement other endeavors. We lay out a research agenda that thoroughly synthesizes principles and methods from multiple distinctive disciplines. The findings of this transformative research will radically change our understanding of (mis)information consumption and mitigation and will trigger a new line of investigation.

Broader Impacts In developing an open knowledge network, it is imperative to ensure credibility—truthfulness, integrity and completeness, since data quality directly impacts the utility of data-driven insights and decisions. A credible open knowledge network will empower several areas of national importance. First, it will become an indispensable data source for debunking misinformation, which is vital to a society struggling with an unprecedented amount of falsehood. Second, it helps secure the cyberspace and protect both digital and real worlds. Third, it can help improve the human condition by transforming healthcare with intelligent computing that promotes and supports health-related decisions using reliable data. Therefore, the project has potential **societal, economic, and educational impact** on a broad range of individuals, governments, corporates, and nonprofits. The project will also provide to a large number of students ample training opportunities, which will aid the development of a diverse and globally competitive workforce.

Multidisciplinary Team for Use-Inspired Convergence Research We are a team of experts in computer science, economics, journalism and communication, political science, psychology, and public health. The **principal investigator** C. Li will work with the four co-PIs (S. Adali, X. Liao, Y. Wu, and J. Yang) and senior personnel to coordinate the project. We continue **team building**. Committed partners include Amazon (Luna Dong), Army Research Lab (Jonathan Bakdash, Laura Marusich-Cooper), Cardiff (Alun Preece) and Duke (Ashwin Machanavajjhala, Lavanya Vasudevan, Jun Yang) universities, Google Research (Cong Yu), IBM Research - Almaden (Marina Danilevsky, Yunyao Li), ICF Inc., a global cybersecurity consulting company (Char Sample), Indiana U. (Xiaojing Liao), NYU (Juliana Freire), Pacific Northwest National Lab (Sutanay Choudhury), Qatar Computing Research Institute (Giovanni da San Martino, Preslav Nakov, Nan Tang), RPI (Sibel Adalı), Temple U. (Jing Gong), UCSB (Miriam Metzger), U. of Maryland (Naeemul Hassan, starting in Fall19), UT-Arlington (Gautam Das, Ming Li, Shirin Nilizadeh, Mark Tremayne, Yan Xiao, Jennifer Zhang), UT-Dallas (Daniel Krawczyk, Lauren Santoro), and Washington State (Yinghui Wu).

The project supports a **multi-institutional multidisciplinary team** that has significant critical mass in areas pertinent to this project, comprised of: 1) leading computer scientists in data-related areas, such as knowledge graphs, data

management, machine learning, NLP, data mining, information diffusion, and web information discovery, security and privacy, and their applications; 2) renowned academics and researchers in psychology, political science, healthcare, economics, and journalism and communication; 3) industrial partners with major contributions to the largest knowledge graph products (Amazon, Google, IBM Research-Almaden) and Google's fact-checking products; 4) healthcare organizations, security industry, fact-checking organizations and other nonprofits; 5) government research arms, such as ARL and PNNL; and 6) international collaborators, such as Cardiff U. and Qatar Computing Research Institute.

PI C. Li and several team members (Choudhury, Danilevsky, Dong, Y. Li, Wu) are well versed in knowledge graph research. Yang, Li and Yu pioneered the field of computational fact-checking. Co-PI S. Adalı serves as the Associate Dean of Science for Research at RPI and leads interdisciplinary research efforts including research on computational models of trust. She has won multiple best paper awards [39, 49, 47, 134]. Co-PI X. Liao directs system security group at IUB. Her research on NLP-based cyber threat intelligence has been awarded NDSS Distinguished Paper Award (2018), ACM SIGSAC Doctoral Dissertation Award Runner-up (2018), and CSAW Best Applied Research Paper Award (2016, 2015). Co-PI Y. Wu directs the Database Lab at WSU. He is a joint scientist at PNNL. His research in distributed database systems and knowledge management has been awarded the ACM Research Highlight Award, a Best Paper Award at SIGMOD conference (2017), and a Google Faculty Research Award. Co-PI J. Yang works on databases and data-intensive systems, with a long track record of collaborating across disciplines, such as ecology, immunology, journalism, and public policy. He co-authored a paper that introduced computational journalism to the database research community and was a winner of Best Outrageous Ideas and Visions Paper Competition at CIDR 2011. Senior Personnel M. Metzger is a leading expert on how users evaluate the credibility of information online. She has published extensively on this topic in multiple disciplines and she edited a book published by MIT Press on digital media and credibility. Senior Personnel Yan Xiao has been awarded multiple NSF grants for research on information technology from the perspective of healthcare domains. His most relevant project (collaborative PI: Xiao, IIS-1838621, 10/18-9/22) is about investigating key strategies to address the current opioid crisis. Senior Personnel Juliana Freire has developed techniques and open-source systems to discover domain-specific content on the Web, including The ACHE Focused Crawler [9], and Domain Discovery Tool (DDT) [17].

Justification for RAISE Funding This project brings together a large multidisciplinary team to pursue a bold research agenda. The proposed research stands at a unique point that converges horizontal research themes (knowledge management, deep learning, AI) and vertical application domains (e.g., health, security) through data-intensive research as a whole, while advances each of its component area with novel core and analytical techniques. The project will improve existing and foster new collaboration and partnerships from multiple disciplines. With the availability of open knowledge network, researchers can conveniently plug in new knowledge and enable knowledge sharing of credible information, and make better utilization of high-value data sources to *accelerate* innovation cycle. Open challenges in security and healthcare, among other domains, can be addressed by this novel and innovative way on top of our credible open knowledge network. The project will also provide a unique and diverse (emphasizing participation by women and underrepresented groups) workforce by training researchers and students for managing multidisciplinary knowledge. The outcome, bridging knowledge management and fact checking techniques to society, will improve the understanding of the critical individual and social activities for end users and general public.

3 Cross-Cutting Horizontal Research Thrusts

3.1 Task A: Data Modeling: Credibility as a "First-Class" Property of Knowledge Graphs

The very first challenges we face are what knowledge we need to capture in order to promote credible information and demote misinformation, and how we should represent such knowledge in a way that enables scalable computational approaches. Existing knowledge bases are often represented by *knowledge graphs*. A knowledge graph G consists of a set of facts (v_x, r, v_y), where v_x and v_y refers to a subject and object entity (node) in G, respectively, and r refers to a relation (edge) between v_x and v_y. While this presentation is general, there remain many technical issues when we seek to make credibility a first-class property of knowledge graphs.

First, knowledge is constantly evolving, and there may be conflicting sets of "facts" until consensuses emerge. A claim once deemed as credible may be disproved later, and sometimes this process may take many years. For example, in the 1920s, 1930s, and beyond, tobacco companies quoted medical research and appealed to the authority of doctors to help suppress public concerns of the harm of smoking. Tobacco advertisements also routinely appeared in reputable journals such as The Journal of the American Medical Association (JAMA), some suggesting prescription of "safer" tobacco brands to patients with sore throats and cough. It was not until the 1950s when the medical community reached consensus on the harm of tobacco, and JAMA banned tobacco ads in 1953. It is therefore critical for our knowledge representation to handle evolving and conflicting pieces of knowledge over time gracefully.

Another modeling challenge is determining the appropriate level of the knowledge that we need to capture. There are many factual statements that can be derived from base knowledge or data—e.g., from historical stock market performance, one can make a statement about its trend in recent years—yet it is infeasible to enumerate and store all such derivative facts in a knowledge base. On the other hand, we need a way to handle misinformation based on such derivative claims, which frequently arises in practice. For example, the claim that "The US stock market is off to its best start of the year since the early 1990s" is factually correct as of February 2019 [24], but the stock market was rising after the "worst December since the Great Depression" [23]. Hence, the implication of substantial growth in early 2019 is misleading. In this case, it would suffice for our knowledge base to store the historical stock market performance but not the derivative facts, but importantly, we need mechanisms for checking such facts using the knowledge base in a way that goes beyond merely testing logical implications (a task that will elaborate later in this section). Clearly, the appropriate level of the knowledge to capture depends on how this knowledge is used. For the pilot phase of our project, we plan to make this determination for each of our target vertical domains.

We also observe that, in order to combat misinformation effectively, we need to go beyond a knowledge base of "true facts." It would be useful to build a corpus of misinformation, and augment it with additional information on how each piece of misinformation misleads its audience and how it was originated and propagated. There are various signals that are indicative of misinformation [3], ranging from the use of click-baiting titles, cherry-picking numbers in claims, to selectively citing studies that are outdated or funded by entities with conflicts of interest. Capturing this rich set of signals offers many advantages over simple binary true-or-false verdicts. First, as illustrated earlier, many claims (e.g., factually correct claims that cherry-pick) do not have binary truth labels. Second, identifying those signals prevalent in a piece of misleading information allows us to generate better explanations for why it is misinformation, and better defenses tailored toward these specific signals. Third, by making these signals specific, we have better hope in developing specific computational techniques for detecting each signal automatically. In the pilot phase of this project, we will refine these signals, and manually identify such signals for a subset of our misinformation corpus. Our eventual aim at the conclusion of the second phase of the project is to be able to train machine learning models that can automatically label new contents with such signals. The pilot phase will focus more on designing and evaluating these signals, to see whether they can be reliably measured (by evaluating inter-rater correlation, for example), how costly they are to label manually, and if any automation techniques are feasible.

3.2 Task B: Data-driven Understanding of Persuasiveness of Factual Claims and Effectiveness of Intervention Mechanisms

This task aims to answer three questions 1) what factors make people accept a (false) claim, more specifically what contributes to the persuasive power of factual statements; 2) how can credibility be gauged, e.g., what signals are more effective than others in establishing truthfulness? and 3) how to persuasively explain the verdict on a factual claim from an algorithmic fact-checking tool (such as the ones that will be developed in Task C.2). The examination of these questions will be guided by cognitive and communication principles.

While questions 1) and 2) have been looked at in conventional psychology, political science, and communication studies [116, 64], this research is a departure from that, due to our data-driven focus and approach. Particularly, our analysis of the persuasiveness of factual claims will take a fine-grained, structured approach. For instance, in our preliminary investigation we conducted informal interviews in which we ask people to compare two simple statements (e.g., S1: "He is the only student in the department that speaks French" vs. S2: "He is the only student in the department that speaks French and plays Ping Pong") and decide which statement impresses them more. A majority of the interviewees chose S2. It appears many people tend to be impressed by stacked conditions. They fail to recognize that one can always become unique after stacking enough conditions together, while it is more difficult to stand out as unique in a group by a single criterion.

Task B.1: Understanding the Persuasiveness of False Claims. Research has demonstrated that false claims can be persuasive for several reasons. First, humans are "truth-biased." The truth bias (or *truth-default theory*) is a human tendency to accept others' statements as truthful. Thus, our first instinct is to trust what we hear or read [68, 90]. Second, research on selective exposure finds that people tend to avoid information that goes against their prior attitudes and beliefs [141]. Algorithmic filtering via "filter bubbles" contributes to this as well [118]. Such instances of selective exposure cause people to filter out information that could help them recognize and disconfirm falsehoods because they get few contrasting views to counter misinformation [91]. Third, research on motivated reasoning shows that even when facts are not filtered out through selective exposure or filter bubbles, they are often interpreted in different ways by different people: Individuals engage in goal-directed processing of new information to protect their preexisting attitudes, values, and ideologies [116, 141]. Additionally, individuals in these homogeneous and polarized social

groups are rarely exposed to opposing views, making them even more vulnerable [99, 54, 41]. Moreover, when these sorts of directional goals influence reasoning, individuals are prone to the "confirmation bias," which is the tendency to privilege information that is consistent with our predispositions and discredit information that appears contradictory.

Finally, according to the Elaboration Likelihood Model (ELM) theory of persuasion [121], there are two distinct levels for evaluating information. The rational level involves deliberate reasoning and is used to test the veracity of the information. The emotional or heuristic level entails more automatic processing, general positive and negative impressions of information (e.g., whether information is relevant and is in sync with one's opinions). Because the emotional level is often fast and effortless, it is particularly compatible with the passive news and information consumption patterns that are common in social media, a primary source of news for many individuals. The ELM suggests that factual content has a role in persuasion but that other message characteristics can impact a user's attitude toward the message in positive or negative ways. While research shows that careful, analytical thinking helps buffer against believing false claims, most people tend to be cognitively lazy [120]. Research by team member Metzger's project team finds that people are unlikely to exert much effort to evaluate claims they encounter online, opting instead to use quick and simple heuristics such as source familiarity or social endorsement cues (e.g., "Likes") [100]. These things make debunking false claims difficult.

We will collect additional data in experiments described in Task B.2. below using multiple choice and open ended questions. These experiments will seek to better understand the conditions under which participants are more likely to believe a true or false claim and whether or not the use of an unbiased, natural language tool developed by the team in this proposal is successful in combating false claims.

Task B.2: Interventions for Combating Misinformation. Prior work on interventions for debunking false information offers a number of suggestions such as providing alternative account/explanation, emphasis on facts, simple and brief rebuttal, and affirmation of worldview [91]. Prior studies recommend addressing gaps by concentrating on facts rather than the myths, repeating the facts and providing them as part of a coherent story. There are some unique challenges presented by using automated tools for this purpose. Research shows that users have a quicker decrease in confidence in algorithmic forecasters over human forecasters when seeing the same mistake occur [55]. This notion of *algorithmic aversion* means that for any automated tool to have an impact, it also needs to be trusted. Furthermore, while providing explanations helped information consumers understand how a system works, it did not always help them make better decisions [126, 86]. In fact, too much explanation may erode trust. Given that news consumers may not rely on evaluation of facts in their evaluation of information [121], detailed explanations in debunking information may also not be equally effective. The news context of misinformation provides additional challenges as news stories may contextualize and decontextualize claims [82, 88]. A single story may have many misleading claims and may employ highly emotional language aimed to appeal to heuristic evaluation of the information. Furthermore news consumers may or may not be familiar with the specific topic of the claim, such as the link between vaccines and autism, and hold strongly held beliefs regarding this topic. Debunking claims in highly entrenched narratives may be less effective and lead to erosion of trust with the underlying tools. Team member Adalı's prior work shows that there are significant differences in the acceptance of AI assistance regarding news [82]. While some users improve with assistance and even more so with explanations, other users are helped more with simpler credibility scores and some users are not helped much at all. These results suggest that interventions for debunking claims may need to be tailored to specific individuals and/or groups. The customization of feedback can be both by the level of feedback provided from black box ratings to highlighting misleading statements or providing detailed explanations as described above. Furthermore, the explanations may be provided by default or can be shown if the user requests it.

To test the effectiveness of using knowledge graphs to debunk false or misleading claims, we will conduct extensive user studies using real stories sampled from the NELA datasets published by Adalı's group featuring more than one million news stories from a variety of sources [81, 114]. We will design and implement user studies using a crowdsourcing marketplace (such as Amazon Mechanical Turk) that has been shown to provide access to sufficiently diverse populations in terms of age, news literacy, and political opinion. Using randomized between-subjects experiments, we will test two basic hypotheses: *H1: The method of presentation of debunking minformation impacts its acceptance* and *H2: The continuous use of a debunking tool will improve participants' reliance on the tool in decision-making.* To test these hypotheses, we will ask participants to rate the reliability of articles with and without debunking feedback. The feedback type will be varied between (a) a single rating mechanism for the article or the source, (b) highlighting of incorrect claims, or (c) providing an explanation of why the claim is wrong, such as by stating a fact that contradicts the claim in the article. In our initial study, we will ask participants to rate a small number of articles for a specific type of feedback mechanism. In our follow-up study, we will explore the repeated use of the same feedback mechanism, allowing participants to rate multiple articles with the same feedback type. We will also evaluate

the potential for group-level variations (e.g., social, demographic, media consumption patterns, and other factors) for effective customization of feedback based on our studies.

To control for the impact of prior opinions on decision-making, we will carefully select topics as case studies and measure participants' current opinions on a given topic via a questionnaire administered prior to the experiment. We will also collect information regarding participants' level of news literacy and trust in specific sources similar to our prior work [82]. We will also collect post-experiment data on participants' perceptions of the debunking method used.

3.3 Task C: Vetting Factual Claims using Credible Open Knowledge Network

Task C.1: Claim Verification Through Querying Knowledge Graphs. This task considers vetting factual claims through querying the knowledge graphs. This entails translating a claim into one or more associated queries. If a query checks out, we can potentially verify a claim fully automatically. Even if such a goal cannot be achieved for a claim, partial results are still valuable. The query may not directly correspond to the claim, but further manual processing of its result may lead to conclusion regarding the claim's veracity.

This research task can be decomposed into several key challenges. 1) To help understand factual claims, we will develop domain-agnostic and domain-dependent taxonomies and templates of factual claims. For instance, one such template is so-called *prominent steaks* (e.g., "The Nikkei 225 closed below 10000 for the 12th consecutive week, the longest such streak since June 2009.") which can be abstracted as a measure over/below a value x for a consecutive period y, as studied in C. Li's prior work [160, 84]. In fact, several team members (C. Li, Hassan, Yang, Yu) have also developed algorithms and an integrated system FactWatcher [76] for discovering facts following this and other templates, including *situational facts* [140] and *one-of-the-few facts* [150]. 2) For generating structured representation of factual claims, we will extend and develop linguistic frameworks to capture factual claims' linguistic and semantic structure. C. Li's group recently proposed an extension to FrameNet [38] by adding 15 new frames specifically for modeling factual claims using frame semantics [37]. 3) We will apply semantic parsing, entity resolution and relation recognition tools for matching factual claims with entities and relations in knowledge graphs. In our preliminary work, we are corroborating WikiData relationships with Wikipedia sentences in order to identify different ways of describing a relation. For instance, "x graduated from y" and "y is x's Alma Mater" are two different ways of conveying the same information. Identifying such rephrasing patterns will allow algorithmic solutions successful on one claim template to also work on its alternative templates. 4) Finally, for vetting factual claims, we will produce algorithms to translate the claims into structured queries over knowledge graphs, by exploiting a multi-modal approach that takes into account the aforementioned claim templates, structured representation of claims using frames, and matching between claims and knowledge graph nodes and edges.

Task C.2: Automatic Explanation of Verification Results. We will devise methods to automatically generate explanations of the process and verdicts used by our algorithmic tools, including the role of knowledge graphs in them. The design and implementation of these methods will be grounded in social science theories and our findings from Task B regarding the persuasiveness of both factual claims and explanations of vetting results. Additionally, a growing body of research into decision science as well as behavioral science and cybersecurity suggests that values held by various actors may provide insights into creators, disseminators and targeted victims [70, 71, 45, 44, 80, 113, 79, 147, 63]. These work will be leveraged to deliver explanations to users that incorporate lineage and provenance information from the algorithmic tools developed in this project.

For instance, PolitiFact recently fact-checked the claim [13] "D.A.R.E. removed cannabis from its list of gateway drugs." Consider a knowledge graph containing nodes representing entities including organizations such as D.A.R.E. and substances such as cannabis, as well as edges connecting D.A.R.E and such substances, representing gateway drugs on their list. To debunk the above claim, a tool can present to its audience the portion of the graph that captures this list and point out that cannibis is still on the list. This explains the source of the data and the method adopted in fact-checking the claim. Such explanations can come in several forms. In its simplest fashion, the explanation can provide links to data sources, including both the knowledge graph and the source dataset where the knowledge graph ingested information related to the claim. Taking it one step further, the explanation can present the graph itself by visualizing it with the initial focus on the relevant nodes and edges, allowing a user to interactively explore the graph. Furthermore, a textual summary of the evidence can be automatically generated.

Debunking a claim is more subtle than whether the data check out. Consider again the example from Section 3.1: the claim "The US stock market is off to its best start of the year since the early 1990s" is true if it is taken literally (as of February 17 2019, when the article with the aforementioned headline was published [24]). However, the stock market was rising after the "worst December since the Great Depression" [23]. Hence, the fact about the substantial growth in early 2019 was established using a particular time window and is not universally robust when

it is considered under different windows. A team led by Yang, with the participation of Li and Yu, has pioneered a computational approach called perturbation analysis [151, 152, 158] towards debunking such quantitative claims. In a nutshell, making such a claim amounts to evaluating a function over some underlying data (e.g., historical stock market performance in this case), but this claim's specific setting of the function parameters (e.g., the window of comparison) controls what view of the data to present, which can be partial and misleading. Perturbation analysis involves tweaking the parameter settings and re-evaluating the same function to see where the original claim's conclusion stands relative to this much larger context consisting of alternative viewpoints. This approach allows us to formulate various fact-checking tasks—e.g., disambiguating claims, assessing robustness and uniqueness of claims, and generating counterarguments—as computational problems that can be solved algorithmically. In our earlier work, we have developed a public-facing website for the 2016 elections that allowed fact-checkers and citizens alike to apply perturbation analysis to claims on the voting records of the members of the U.S. Congress [144, 143]. In this project, we will explore how perturbation analysis can help generate effective explanations for our target vertical domains, with not only succinct textual counterarguments but also more natural narratives as well as visualizations. For instance, for the stock market claim above, we can visualize the stock market's performance in both early 2019 and the period before it side-by-side; a textual summary correspondingly should contrast the two periods.

3.4 Task D: Improving Credibility of Knowledge Graphs

Task D.1: Erroneous Fact Detection and Repairing. Real-world knowledge bases are often dirty as they are automatically extracted from data sources. Existing data repairing methods [72, 52, 142, 138], including our prior study on data cleaning systems [59, 53] assume rigid schema to correct erroneous values to conform to predefined constraints. We will develop outlier detection algorithms for finding potential erroneous facts and data cleaning methods for automating the correction of inaccurate facts.

For *error detection*, one idea is to extend C. Li's recent work Maverick [161, 162], which is a graph mining system for discovering exceptional entities from knowledge graphs. An entity is considered exceptional is it possesses some peculiar attribute values that make it stand out among a context of entities of the same type. Such outliers could be due to erroneous data and thus serve as cues for locating the errors. We plan to extend Maverick in several directions, including making it feasible for efficient error detection over a massive graph, through computation sharing across similar entities and parallel mining algorithm exectuion, as well as making it usable so as potential errors are detected together with insightful explanations. With regard to *error repairing*, consider a set of erroneous facts (edges) in a knowledge graph G ranked by an exceptionally scoring function f, a set Σ of graph editing operations (e.g., change attribute values, add/remove edges), and an editing cost function (e.g., graph editing distance) [66]. Following minimum repair model [36], we want to solve the following optimization problem: compute a new graph G' by applying operators from Σ that incurs minimum editing cost and maximally reduce the exceptional scores of the revised facts in G'. We will study the hardness and approximability of this problem. (1) Different repairing actions interact with others: Correcting node attribute may create new erroneous facts or fix existing ones. In response, we plan to use auxiliary structures such as *error dependency graphs*, which dynamically track the errors (as nodes) and their interaction (as edges), and are dynamically maintained by incremental error detection following Task 2.1. (2) To reduce the computation cost, we will investigate beam search with backtracking [164] to dynamically monitor the current optimal repairs and prune unpromising repairing sequences, while backtracking avoids incomplete search.

Task D.2: Inferring New Facts to Evolve Credible Knowledge Network. This task investigates a repertoire of approaches for bootstrapping and continuously growing and curating the credible open knowledge network. Existing predictive models infer new facts to complete partial knowledge bases with rule models (in the form of $X \Rightarrow Y$ with condition X and facts Y) or representation learning [119, 112]. The PIs' preliminary study has developed several expressive computationally efficient subgraph pattern models to extract event from News [51], cyber attacks [137]; financial activities [109] among other applications. Our key idea is to *enhance conventional models by incorporating instance-level features captured by expressive subgraph pattern models*,

Rule-based fact inference. We propose enriched rule models by incorporating subgraph features characterized by *credible scope*. A credible scope $P(x)$ is a subgraph pattern that carries a set of node variables x, and extracts credible subgraphs from validated fraction of knowledge graphs. A rule enhanced with credible scope is in a general form of $P(x), X \Rightarrow Y$, where its conventional counterpart $X \Rightarrow Y$ is a rule conditioned over subgraphs that matches $P(x)$ by e.g., subgraph isomorphism. One example is to verify data breach caused by masked attacks [136]. A masked attack starts with a Distributed denial of service (DDos) as a diversionary tactic to "mask" other cyber crime, including information stealing. An example of a rule that verifies a claim "*the data breach at a victim*

server is caused by a masked attack" is illustrated in Figure 1. We will study two problems. (1) Identify expressive, domain-specific models to characterize credible scope P in connection with news, finance, health and security applications, such as subgraph models with quantifiers (e.g., "connect to more than m bots") and temporal constraints. (2) Devise supervised learning techniques to discover rules from training facts. Given a set of true and false facts, one method is to integrate supervised pattern mining [115] and domain-specific subgraph models to adaptively discover the rules that best distinguish credible facts from the false ones. We will also develop optimization techniques to scale rule learning and inference to large datasets such as graph sampling and compression [83].

Deep Knowledge Inference. Deep models such as convolutional neural networks fall short in tasks over non-euclidean data such as attributed networks. Static models do not make full use of true information that benefits fact prediction. PIs' preliminary study [94, 137] observe that real-world facts can often be better jointly modeled by entity attributes and topological features. We will explore deep knowledge graph representation model by extending graph convolution neural networks (GCNs) [154] with propagation models. Examples of enriched node features can be sampled path features [148], subgraph features [67, 94], or embeddings from domain-specific vocabularies [43]). Specifically, each edge (fact) is associated with a "fact node" with a binary flag ("true" or "false"). The model update at entity v (with hidden state h_v^i) is defined as ($i \in [1, m]$ for m layers): (1) $h_v^0 = F(v)$, (2) $h_v^i = \mathrm{ReLU}(W_i \sum_{u \in N(v) \cup v} \frac{p_{(u,v)}^{i-1} h_u^{i-1}}{\sqrt{|N(v)||N(u)|}} + B_k p_v^{i-1} h_v^{i-1})$ where ReLU is a rectified linear unit function, and W_k and B_k are the model parameters to be learned. The influence p_v^{i-1} measures how the entity information of entity v at layer $i-1$ affects its counterpart in the layer i. The structural influence $p_{(u,v)}^{i-1}$ captures the influence of the features of the neighbors u of v to the local information of entity v. The goal is to learn GCNs (a binary node classifier) for the fact nodes. We will develop efficient learning algorithms and verify the effectiveness of the deep inference models. Co-PI Wu has collaborated with Xin (Luna) Dong on fact summarization over knowledge graphs. We will consult our partners from industry and other application domains to ensure the effectiveness and quality of our inference methods.

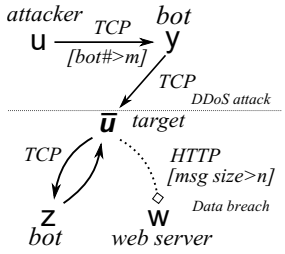

Figure 1: A rule that verifies data breach masked by DDoS. The credible scope validates DDoS co-occurred with a data breach at victims, bots and Web servers identified by variables $\bar{u}$, z and w.

4 Vertical Application Domains

While conducting research in the cross-cutting horizontal areas, our focus will be particularly on several application domains, including public health and security. During Phase 2 of the project, we will also investigate the finance application domain, following ongoing discussion between several team members, including Y. Li and M. Danilevsky at IBM Research - Almaden and C. Li. Particularly, Y. Li's team at IBM has developed Content Service [42], a system that constructs a scalable knowledge base in the finance domain from a variety of data sources, including reports filed with the SEC (for public companies) and FFIEC (for FDIC-insured banks). Claims of financial nature or financial statements made by a company's spokespersons (e.g., "Last quarter we sold more cars than any of our competitors.") can be possibly fact-checked against the knowledge base.

4.1 Health

Background: Misinformation in health is common and can arise from a variety of sources, including knowledge gaps, intentional manipulation ("disinformation"), and beliefs based on outdated, incorrect, or insufficient knowledge sources. Misinformation can lead to serious public health consequences, such as vaccine-preventable disease and opioid addiction epidemics. Two experts in health services research (Xiao and Vasudevan) will lead health domain research based on their synergistic activities. Our project will apply intelligent computing using open knowledge networks from different sources of data to combat spread of misinformation related to two high priority public health challenges—vaccine hesitancy and opioid crisis.

Vaccine Hesitancy: Globally, the coverage of childhood vaccines has stalled at 85% [26] with 1 in 10 infants were unvaccinated in 2016 [1]. The ongoing measles outbreak in the United States in an example of an eliminated vaccine-preventable disease that has since resurged in hesitant and unvaccinated communities. Misinformation including false claims about vaccines give rise to vaccine hesitancy: parents' decision to refuse or delay vaccines for their children out of concerns about the safety of vaccines and reduced trust in vaccines and vaccination programs. The World Health organization has named vaccine hesitancy as one of the top 10 threats to global health in 2019 [5]. Combating misinformation is key to mitigating parental concerns resulting in hesitancy.

Opioid Crisis: Opioids are high risk medications for preventable patient harms [122]. Misuse of prescription opioids is a serious public health problem in the United States. In 2017, an estimated 18 million people (more than 6 percent of those aged 12 and older) have misused such medications at least once in the past year [65], and an estimated 2 million Americans misused prescription pain relievers for the first time within the past year. Misinformation about the addictive properties of prescription opioids and the misbelief of prescription drugs less harmful than illicit drugs are identified as possible contributors opioid crisis [149, 123].

Challenges: Vaccine hesitancy and opioid crisis pose a number of difficult challenges. (1) Effective communication. Studies have shown that parental concerns about vacinnation vary by contextual influences due to e.g., historic, socio-cultural, environmental, health system, economic or political factors, individual and group influences (e.g., arising from personal perception of the vaccine or influences of the social/peer environment), and vaccine/vaccination-specific issues (directly related to vaccine or vaccination) [98]. For communication to be effective, it needs to be informed by contextually-relevant parental concerns, tailored specifically to mitigate those concerns, and personalized to match individual characteristics using principles of persuasive communication. (2) Addressing potential ethics issues—racially stereotyped intervention could be as bad as (if not worse than) one-size-fit-all intervention that is only effective for the majority population. In general, health related interventions must be considered in the context of patient autonomy and liberty [57], and in the context of patient and family-centered conversations between healthcare consumers and healthcare professionals. (3) How to discern the veracity of claims using data? Voluntary reporting sources on medicines and vaccines such as WHO's adverse event reporting system VigiBase [133] and the FDA database of adverse event reporting (FAERS, part of data.gov) can reliably identify adverse effects (e.g., [163]) despite the concern of underreporting [34]. We can use these datasets to debunk misbeliefs (e.g., that prescribed opioids do not cause addition like illegal opioids [149]) by showing reports of adverse effects. Such data sources have data quality issues, e.g., manipulation through self-reporting false incidents. There is also the danger of misrepresenting numbers derived from such databases, which may be factually correct but still misleading, as discussed in Section 3.1. (4) A fourth challenge is how to handle evolving and potentially conflicting knowledge such as evolving claims [56].

Proposed Research Tasks.

Knowledge modeling: We will identify types of knowledge needed for building effective defense against misinformation on vaccines and opioids, and devise appropriate knowledge representation that enables efficient computational approaches. 1) We will develop a flexible knowledge representation that can handle evolving and potentially conflicting views concerning vaccines and opioids. 2) We will refine various domain-agnostic signals that are indicative of misinformation [3], with a particular focus on misinformation that is based on raw data or cites scientific literature. 3) We will identify domain-specific concerns and issues that arise in misinformation on vaccines and opioids. For example, there is existing literature on issues invoked by anti- vaccine arguments [135, 7, 2, 6, 4]. We will investigate how to identify such issues algorithmically, e.g., by clustering anti-vaccine articles to find latent topics.

Bootstrapping & curating the knowledge base: 1) We will start with a manually curated set of medical facts on vaccines and opioids, leveraging existing sources such as cdc.gov and vaccines.gov. We will develop plans for building partnerships for future phases of our project to develop automated techniques for knowledge graph construction from primary biomedical literature, based on the demonstrated feasibility of automated approaches such as KnowLife [58]. Work in future phases will include extending existing techniques to handle evolution of knowledge and to track the lineage of such knowledge to research articles and studies. 2) To help assess claims based on raw data, such as FAERS and VigiBase, we will develop outlier detection on incidents of adverse events associated with vaccines and opioids, to find potential misreporting. 3) To construct a repository of misinformation on vaccines and opioids, labeled with both domain-agnostic signals and domain-specific issues, we plan to investigate machine learning techniques for automatic labeling. We will build upon existing work of Hassan's group on automatically labeling the quality of health news using 10 established criteria. In that work, we developed a manually labelled dataset from healthnewsreview.org with more than 6000 health-related news articles. Preliminary experiments show that using word, parts of speech tag, entity features, a support vector machine (SVM) algorithm achieved an F1-measure of 0.858 on the 10 criteria on average.

Using the knowledge base to verify claims: 1) We will apply semantic parsing and entity and relation recognition techniques to help understand specific claims, and apply machine learning techniques to identify domain-agnostic signals as well as domain-specific issues in articles. Going beyond linguistic features, we will consider contextual information (such as temporal and geopolitical contexts) surrounding a claim as additional features to improve accuracy. 2) We will apply perturbation analysis techniques [151, 152, 158] to help expose claims that may be factually correct but still misleading, as discussed in Section 3.3. Such techniques will go beyond simple true-or-false verdicts. For example, the claim that there have been about 180,000 reported adverse events for the DTaP vaccine is factually correct [8], but

it can make a misleading impression when presented without a larger context, e.g., how many vaccines were given since worldwide reports started decades ago, or how this ratio compare with other treatments widely accepted as safe.

Effective intervention 1) The ability to pinpoint domain-agnostic signals and domain-specific issues in misinformation, as discussed above, makes it possible to generate persuasive explanations and arguments directed against each specific instance of misinformation. In the pilot phase, we will develop a prototype system that can automatically generate and deliver such interventions in real-time. Our project team pioneered live automated "pop-up" fact-checking for broadcasting events [29, 30]. We have also been developing browser plugins that detect misinformation by matching contents of web pages against a database of "myths" collated from authoritative sources such as CDC. Building on these delivery mechanisms, in Phase 2, we will incorporate explanation and arguments more directed towards specific signals and issues. 2) We will start to formulate approaches for acquiring profiles on how individuals have been exposed to and influenced by vaccine or opioid misinformation, and for using these profiles in generating more personalized interventions. For example, suppose that an individual has been exposed to an anti-vaccine article that invokes religious objections and cites debunked studies, and the individual is not likely religious, an effective intervention can then focus on refuting the citations. We also plan to connect our communication-related research with existing best practices in patient communication, such as motivational interviewing [102]. We plan to acquire the individual profiles and implement automated personalized interventions in the next phase of the project. 3) For outreach and team-building, Duke will host monthly meetings during the pilot phase with invited domain experts, including healthcare professionals, educators, as well as patient and public health advocates, to discuss intervention ideas and plans for implementing them in the second phase. These meetings will be facilitated by our project consultant Vasudevan, a faculty member at Duke Family Medicine & Community Health, and Global Health, who is an expert on vaccine hesitancy as well as implementation and evaluation of interventions to improve maternal and child health outcomes.

4.2 Security

Background. *Cyber Threat Intelligence* (CTI) is a collection of information that details current and emerging security threats [129]. Such knowledge is essential for an organization to gain insight into the fast-evolving threat landscape, to timely identify early signs of an attack and the adversary's strategies, tactics, and techniques, and to effectively contain the attack with proper means. Given its importance, CTI has been aggressively collected and increasingly exchanged across organizations, often in the form of *Indicators of Compromise* (IOC) [117], which are forensic artifacts of intrusions such as virus signatures, IPs/domains of botnets, MD5 hashes of attack files, and so on.

IOCs can be extracted from traditional blacklists, e.g., CleanMX [12] and PhishTank [22]. However, they only cover a small number of IOC classes (i.e., URL, domain, IP and MD5). The relationship between IOCs is not revealed and no context information is provided (e.g., the criminal group behind malfeasance). Recently, other sources of information, such as technical blogs [92], review websites [87] and social media platforms [130, 131, 35, 46] have been utilized to extract information about security vulnerabilities and their exploits. For example, Recorded Future is reported to utilize over 650,000 open technical blog sources in 7 languages to harvest IOC [127]. These sources usually have comprehensive descriptions of attacks, and they provide a unique understanding of security and privacy issues of software, applications, and devices from users' perspective.

While these sources have accumulated massive data, there is growing concern about their information quality and consistency. More specifically, as reported in Co-PI Liao's prior work [92], the IOC listed on technical blogs can be incomplete or outdated, leading to false attack detection in intrusion detection systems. Even worse, adversaries were found to extensively spread fake IOC in technical blogs to mislead security practitioners for threat forensics.

Current quality investigation of IOC relies mostly on community effort. In particular, security researchers reconstructed attack processes and then compared the IOC collected in real-time attacks with those in blogs. In a preliminary study, Liao investigated the qualities of malware-related IOC from technical blogs. Particularly, they ran the malware samples mentioned in the blogs in a sandbox and then recorded all the system and network behaviors triggered by such malware samples. They found erroneous network and system related IOC in technical blogs, e.g., missing digits of malicious IPs, false DNS information and incomplete modified register keys.

Approach. Our preliminary study demonstrates the prevalence of misinformation in open web sources of cyber threat intelligence. Current techniques have limited capabilities in capturing such misinformation. More specifically, the preliminary method is focused on investigating malware-related IOC, because their ground truth can be generated. In the meantime, large portions of cyber threats (such as real-time targeted attacks or botnets) are hard to reconstruct and replay, since their attack scenarios are sophisticated and the attack tools and context information are unavailable. We **propose** to bootstrap and constantly evolve a credible cyber threat knowledge graph. Given the knowledge graph, security practitioners can debunk misinformation in the open web sources of cyber threat intelligence by investigating

activities related to malicious events via querying the knowledge graph. As a prominent example, given a technical report mis-describing an attack campaign's DNS information, a security practitioner can query the knowledge graph to retrieve the attack campaign's network information such as autonomous system, hosting IPs, etc.

Proposed Research Tasks. We elaborate our research tasks as below:

Cyber Threat Knowledge Collection : The goal of this task is to combine the data obtained from traditional sources, including CleanMX [12], PhishTank [22] and National Vulnerability Database [21], with the data obtained from technical blogs and social media to create an open knowledge graph of IOCs. Note that, PI Liao developed a tool iACE [92] which uses graph mining to extract individual entities from documented attack instances and their relationships. Such entities and relationships can serve as a basis for identifying the concepts of cyber threat knowledge graph. The traditional sources, e.g., CleanMX and PhishTank, that do not reveal the relationship between cyber threats can be used to label the additional *source* field of the IOCs extracted for multi-source information cross validation (see details below).

Credible Cyber Threat Knowledge Graph: We will extend iACE's learning algorithm for malicious event discovery. Specifically, we plan to extract a 5-tuple event representation (*entity*, *activity*, *timestamp*, *type*, *source*), where entities represent actors in cyber threats, activities represent their relationships, timestamps establish the time sequences of their interactions based upon the relationships, the type specifies the nature of an event, and the source indicates the information resource of the event. To ensure a credible knowledge graph, each event will be evaluated (such as investigating the reputation of source and cross-matching events from multiple sources) before adding it to the knowledge graph. The events extracted by iACE can be used to build a "seed" knowledge graph, by linking different events associated with concepts based on their common entities or types. Given the seed knowledge graph and newly-gathered cyber threat events, we can use word embedding techniques [40, 103, 104] to measure the semantic similarity of the newly-extracted event type with those already in the knowledge graph to learn new events, making the knowledge graph evolve. This approach and other techniques will be investigated in the project.

Using the knowledge base to verify security and privacy threat claims: We will utilize various public intelligence sources, such as leading technical blogs, forums (e.g., Google groups, Security Focus, etc.), research articles from leading security and privacy venues, and social network posts. Liao's group has collected over 71,000 articles from online blogs. We plan to extensively crawl online forums, social networks, code sharing platforms, and other relevant sources.

5 Ethical Considerations

The last several years have witnessed a substantial growth in computational fact-checking with various data-driven and AI-powered tools. But the misuse of AI is manifest in this arena as well, posing an ongoing challenge to fact-checking. Creators of disinformation may use algorithms to generate false content that maximizes the chance of going undetected. Similarly they can automatically generate claims that are factually correct but nonetheless misleading. Tackling the ethical issues raised by the use and misuse of AI is part of our project. This project seeks to arm citizens with tools to push back against a tide of misinformation across many domains, including, health, finance, and security. It requires providing people with reliable information against which new claims can be checked. A similar role has been played by the press for centuries but the scale of the misinformation problem in the social media era is challenging old practices. That said, we can learn from research in journalism and other fields how trust from information receivers can be gained or lost, and we will incorporate best practices into the design of our algorithmic tools.

Echoes of the "Yellow Journalism" period of 125 years ago, where news was marked by sensationalism, exaggeration, partisanship, and fake news [105] are evident in today's media environment. To pivot from Yellow Journalism, in the twentieth century the newspaper industry turned toward objective reporting and a set of principles to win back readers' trust, including accuracy, fairness, transparency, and accountability. These are outlined below along with an explanation of how these lessons are incorporated into our design.

Accuracy. Walter Lippmann believed the foundation of a functioning democracy rested on the quality and veracity of the information citizens consumed [96]. Accuracy is ensured by, first, using high-quality sources of information. Sources should possess subject matter expertise and be situated close enough to the matter being investigated to have access to first-hand information. Second, multiple sources should be used rather than a single source as veracity is increased when distinct sources agree. Finally, information from sources with competing viewpoints should be sought and compared. Accordingly, our project will seek accuracy by relying on multiple and varied high-quality information sources for collecting and preparing our knowledge graphs.

Fairness and Impartiality. Presenting information objectively means emphasizing facts more than opinions, and accurately depicting multiple points of view on a topic. The International Fact-Checking Network (IFCN) has a commitment to non-partisanship and fairness as a first principal for membership [28]. These ideas will form the

basis of the knowledge graph we develop, as the fact-checking tools designed for this project will operate based on algorithm-based matches or mismatches rather than case-by-case human judgment. As such, team members will have to be alert to the introduction of bias in the algorithms underlying the knowledge networks used to adjudicate claims. Having a large team with varied backgrounds is one safeguard being employed in this project.

Transparency. Transparency of information sources and the processes is another key ingredient of credibility. The IFCN has also made transparency a critical requirement for organizations seeking to join. In our project, transparency will be pursued by making users of our tools aware of the data sources used to create those tools and explanations of how specific factual claims were adjudicated. A central challenge for this project is that the verdicts are hard for readers to trust if they cannot see inside the black box and understand specifically *why* a fact-checking tool supported or refuted a claim (see section titled "Automatic Explanation Generation" above).

Accountability. Accountability involves taking responsibility when errors are made, reporting these mistakes and making changes in procedures to prevent similar mistakes in the future. The IFCN requires members make a commitment to this principle. We will pursue this by field testing our tools as part of the development process and publishing a record of successes and failures. We envision this project as a dynamic process. The use of AI in misinformation campaigns makes this particularly important, as fact-checking is often a cat-and-mouse game.

Credibility. Each of the above principles work together to enhance the credibility of any effort to provide people with accurate information. Public perception is critical to this process. Message credibility is enhanced by thoroughness - by receiving not only the verdict of the fact-checking but having an complete understanding of the process that yielded the result. How the information is delivered to the public is important as well. Projects like Share the Facts, which will serve as a model for our team, are an important part of this process [27].

Domain-Specific Ethical Considerations. Decisions related to health and finance are personal, and information designed to induce behavioral changes needs to be considered in the context of respecting an individual's self-determination and privacy as related to these domains. Self-determination [95] is the principle in medical ethics that it is ultimately the patient who should decide whether or not to accept suggested treatment or care. The principle of self-determination can be applied to financial decisions as well. In counteracting misinformation, ethics issues in these domains are unique in that information presented should be in the best interest of an individual, although respect for individual autonomy is imperative in any presentation of information to consumers. Thus, the tools developed in this project will be designed to strike the delicate balance between facts presented to counteract misinformation, and the individuals autonomy in making decisions about the veracity of claims. For example, rather than filtering out claims/articles deemed as misinformation by our algorithms, our interventions will display tailored advisory information that individuals can rely on to evaluate whether a claim/article is credible or false.

Meanwhile, misinformation found in the security domain, particularly for cyber threat intelligence gathering, directly impacts on the effectiveness of defense mechanisms (e.g., intrusion detection systems). Timely disclosure of cyber threat misinformation is critical. Responsible disclosure is the principle in cyber security ethics that security practitioner who found the cyber threats or security risks should report them to the impacted vendors. Our deliverables include cyber threat misinformation and fact-checking report for responsible disclosure. We will also contact the major defense mechanism vendors and the threat intelligence exchange platform about that cyber threat misinformation.

6 Evaluation, Deliverables, and Management Plan

1) Input Collection from Study Participants and Evaluation

Elicit truthful participant input. Input collection from study participants plays a critical role in this project for collecting labeled data that train our machine learning models, assessing misinformation debunking techniques, and conducting user study for understanding persuasiveness of factual claims and vetting result explanations. We take an incentive mechanism to elicit truthful input. Our key idea is to carefully design rewarding rules such that a participant's benefit is maximized for truth-telling. We will use both crowdsourcing marketplaces such as Amazon Mechanical Turk and Figure Eight and our in-house crowdsourcing system [155, 128]. (1) To address the lack of task ground truths, we will reward a participant according to how their input compares with those from peers. We will test the effectiveness of our incentive mechanism in eliciting truthful inputs. Comparison of data quality will be made with the scenarios when no incentives are provided. (2) To gather reliable data from biased individuals, we plan to first conduct experimental studies regarding the effectiveness of various types of rewards on participants with different profiles. The reward under consideration includes, but not limited to monetary payments, extra credits for particular courses, and substitution for one homework submission. In the pilot phase, we plan to focus on university students of different major backgrounds from the participatory institutions in the project. Questionnaires-based survey research will also be conducted. Based on the analysis results, we will then design incentive mechanisms by providing heterogeneous rewards. Experiments

will be conducted on our developed crowdsourcing system which will be modified to fit the diverse reward scenario.

Evaluation. To evaluate knowledge inference, we will measure (a) the agreement of the collected gruthful knowledge facts and inferred ones among our collaborations and the amount of credible data that have been accessed, explored and used by our collaborators; and (b) the evaluation and rating of the usability and effectiveness of our models from searching, analytics and activeness of involved researchers and workforce. We shall compare the accuracy of our fact repairing and inference with conventional models and real search queries. More accurate answers from repaired/inferred facts indicate higher quality of knowledge inference and repairing. To evaluate the collaborative effort, we will use the following metrics: (1) diversity: involvement of different states, institutions, sectors and ethnic groups, and the gender of participants of our research activities; (2) effectiveness: models and datasets that have been used in practice; (3) collaboration quality measured by the number of collaborators, co-developed proposals, the number and quality of co-published papers, among others.

2) Deliverables. Phase 1 of the project will focus on team formation, research plan development, and proof-of-concept deliverables. This shall provide a solid foundation for pursuing the work in Phase 2, of which the planned **deliverables** include a sustainable ecosystem of datasets, algorithms, software, and stakeholder community for enabling and exploiting credible open knowledge network. Toward the latter stage of Phase 2, the team will move research results into end-user applications and public services, by working with community partners through our team members in industry, governments, and nonprofits.

The PIs have ample experience in creating and maintaining public web-based demonstration systems for their projects. PI C. Li also organized a team to participate in the NSF I-Corps Teams program in 2015 which supported market research and customer discovery for ClaimBuster. The experience prepared the PI for moving research along the path toward commercialization.

Horizontal Thrusts. (1) An automated system for vetting factual claims through querying knowledge graphs, together with discovered claim templates and curated frames for factual claims. The system will be integrated with our current fact-checking system ClaimBuster and Squash, to form a suite of tools for debunking misinformation. The system is also equipped with the capability of explaining its claim vetting results. (2) A general repairing framework that automatically track and repair erroneous facts; (3) A package of algorithms that learn novel rule and deep models from credible information to automatically infer credible facts. When we develop these algorithms and systems, we will accomplish proof-of-concept in Phase 1 while identifying key components to deliver for Phase 2.

Vertical Thrusts: Health. For the pilot phase, we will focus on the following deliverables in the domains of vaccine and opioid misinformation. (1) Representation and schema for knowledge relevant to combating misinformation, including lists of domain-agnostic signals and domain-specific issues, and a compendium of existing datasets and resources. (2) Manually curated knowledge base of relevant medical facts; corpora of misinformation and fact-checking articles, with a large enough subset manually labeled with misinformation signals and issues. (3) Proof-of-concept demonstration of automation techniques for following tasks: (a) identifying domain-specific issues from the corpus of misinformation; (b) labeling a piece of misinformation with domain-agnostic signals and domain-specific issues; (c) detecting potentially misreported adverse events in databases; (d) identifying factually correct but still misleading claims based on raw data; (e) generating explanations and arguments directed against specific types of misinformation. (4) Websites and APIs for above resources. (5) Education and training materials. (6) Partnerships with healthcare professionals, educators, as well as patient and public health advocates.

The datasets and the proof-of-concept techniques above will be extended in the next phase of the project. Upon completion of the final phase of the project, we expect to develop effective personalized intervention techniques against health misinformation, together with sustainable open knowledge networks supporting this effort. Building on the partnerships with healthcare professionals developed in the pilot phase, and with our industry collaborators working at various information platforms (e.g., search engines and social media), we plan to implement and deploy our techniques on real users and evaluate their effects on health outcomes.

Vertical Thrusts: Security. In the domains of security and privacy misinformation, we will focus on the following deliverables. (1) Representation and schema for cyber threat knowledge graph to combating misinformation. (2) Corpora of cyber threat misinformation and fact-checking reports, with a large enough subset manually labeled with misinformation signals and issues. (3) Empirical analysis on the criminal objectives and impact of cyber threat misinformation. (4) Proof-of-concept demonstration of automation techniques for following tasks: timely extraction of cyber threats in security-domain corpora; effectively evolving credible cyber threat knowledge graph; detecting potentially misreported events in the sources of threat intelligence gathering. (5) Education and training materials.

3) Coordination and Communication This collaborative, convergent research effort will be managed by PI Chengkai

Li, with the assistance of a project manager (TBD). Multiple team members are located at UT Arlington. Teaming agreements are in place to ensure the participation of subawardees, consultants and collaborators. Implemented during the proposal preparation stage, the team will continue to use Microsoft Teams for video conferencing and instant messaging, with "channels" designated for key topics. The team will use the following methods to coordinate effort, maintain communication among participants, and mitigate risk of technical challenges disrupting the project:

Kick-off Meeting: The PI will hold a kick-off meeting (in Microsoft Teams) within 7 days of award to review the project management plan with the team.

Team Meetings: The team will assemble as a group and discuss project progress from the previous periods' work, describing how new results contribute to required milestones and discussing any challenges that arise. A whole-team in-person meeting be held in Arlington, TX, in the middle of Phase 1, for discussing project progress and planning for the blue-ribbon presentation and Phase 2 proposal.

C-Accel Cohort Meetings: $30,000 are budgeted for supporting 5 team members each time to attend three in-person NSF-sponsored training workshops for the Convergence Accelerator Program.

Progress reports : On a monthly basis, the PI will request a summary of work completed and in progress at each site, milestones met, problems encountered, updates to the program schedule, financial status, and remaining work.

7 Integrating Proposed Research with Education

Student training. Due to the broad nature of our research efforts, we will also promote workforce education by developing training materials appropriate for students from computer science, communication and journalism, economics, political science, psychology, and public health. For example, the Duke team working on health misinformation plans to develop educational materials that teach students and citizens alike how to defend themselves when presented with misinformation. Such materials would include lists of known reputable and biased sources, domain-specific issues often invoked by misinformation, and explanations of various signals indicative of misinformation, together with concrete examples. The materials will also include exercises where the learner applies the lessons learned to label some specific pieces of information. Not only do these materials have educational value, but responses from learners will also help the project validate its approaches and collect labelled data useful for improving machine learning models.

Curriculum development activities. Results from this project will be integrated into existing and new undergraduate and graduate courses in multiple topics, including courses on programming, databases and data mining at all institutions involved. Such integration will expose students to large datasets of public interest, data science tools and applications, and algorithms for novel data analytics operations. In particular, the UTA team will introduce graphs as non-relational data models to undergraduate databased course CSE3330 Database I, and topics related to knowledge graphs, graph mining, and AI-powered applications exploiting graph data to undergrad/graduate data mining course CSE4334/5334 Data Mining. Discussion of current research directions will also be integrated into graduate seminar course CSE6339 Graph Data Management and Mining. Similar courses at other institutes (e.g., CS415 Big Data/CS580 Advanced Database taught by Co-PI Wu at WSU, CSCI-4380 Database Systems taught by Co-PI Adal at RPI, CS365 Data Analysis and Mining taught by Co-PI Liao) will also follow the same approach.

Plan for Broadening Participation in Computing (BPC). The team members have very strong track record in broadening participation in computing, through mentoring a large number of high school students, underrepresented, female, and undergraduate. The commitment to diversity and our projects' broader societal impact will help us attract talents from a diverse pool – not only those from computer science, but also journalism and public policy. The PI actively participated in UTA's middle/high school outreach programs. The high school team under the PI mentored received the runner-up award in the program's research competition. The PI directs one of the most diverse research groups in the department, including five female and one Hispanic Ph.D. students, one Black M.S. student, and three undergraduate REU students with one African-American. An REU project mentored by the PI has won first runner-up award in the SIGMOD'17 undergraduate student research competition

In addition, the Duke team participates in the Bass Connections, a university-wide program at Duke aimed at providing students with greater exposure to inquiry across the disciplines, sustained mentorship in teams, and the chance to experience the intersections of the academia and the broader world. In the past two years, the team has worked with more two dozen undergraduates on projects related to fact-checking and vaccine misinformation. Besides undergraduates, both Machanavajjhala and Yang have hosted six high school student researchers over the same period. Futhermore, Co-PI Wu serves as a research mentor of WSU LSAMP (LouisStokes Alliance for Minority Participation), an NSF-funded consortium, educating underrepresented minority students in STEM. Co-PI Wu will deliver the research outcome to LSAMP student projects.

References Cited

[1] 1 in 10 infants worldwide did not receive any vaccinations in 2016. https://www.who.int/news-room/detail/17-07-2017-1-in-10-infants-worldwide-did-not-receive-any-vaccinations-in-2016.

[2] Common Vaccine Safety Concerns . https://www.cdc.gov/vaccinesafety/concerns/index.html.

[3] Credibility Signals, W3C Editor's Draft 03 June 2019 . https://credweb.org/signals/.

[4] Talking about Vaccines. http://www.immunize.org/talking-about-vaccines/.

[5] Ten threats to global health in 2019. https://www.who.int/emergencies/ten-threats-to-global-health-in-2019.

[6] Trusted Sources of Vaccine Information . http://www.vaccineinformation.org/trusted-sources/.

[7] Vaccine Safety . https://www.vaccines.gov/basics/safety.

[8] VigiAccess Numbers in Context . https://vaxopedia.org/2018/08/08/vigiaccess-numbers-in-context/.

[9] The ache focused crawler. https://github.com/VIDA-NYU/ache.

[10] ClaimBuster: end-to-end fact-checking. http://idir.uta.edu/claimbuster/.

[11] ClaimPortal: Integrated Monitoring, Searching, Checking, and Analytics of Factual Claims on Twitter. http://idir.uta.edu/claimportal/.

[12] Cleanmx. http://lists.clean-mx.com/cgi-bin/mailman/listinfo/viruswatch/.

[13] D.A.R.E. still thinks marijuana is a dangerous drug for kids. https://www.politifact.com/facebook-fact-checks/statements/2019/may/30/viral-image/dre-still-thinks-marijuana-dangerous-drug-kids/.

[14] Demonstration video of ClaimBuster. https://vimeo.com/188729744.

[15] Demonstration video of ClaimPortal. https://vimeo.com/329947070.

[16] Demonstration video of FactWatcher. https://vimeo.com/154356599.

[17] Domain discovery tool. https://github.com/VIDA-NYU/domain_discovery_tool.

[18] FactWatcher: monitoring of facts from real-world events. http://idir.uta.edu/factwatcher/.

[19] Linking open data. http://linkeddata.org/.

[20] Metpetdb: A Database for Metamorphic Petrology (System). http://metpetdb.org.

[21] National vulnerability database. https://nvd.nist.gov.

[22] Phishtank. https://www.phishtank.com.

[23] Stocks book their worst year since the financial crisis and worst December since the Great Depression. https://markets.businessinsider.com/news/stocks/stock-market-news-on-track-worst-december-since-great-depression-2018-12-1027837251.

[24] The US stock market is off to its best start of the year since the early 1990s. https://qz.com/1552668/the-us-stock-market-is-off-to-its-best-start-of-the-year-since-the-early-1990s/.

[25] This Washington Post fact check was chosen by a bot. https://www.poynter.org/news/washington-post-fact-check-was-chosen-bot.

[26] WHO Fact-Sheet: Immunization Coverage. https://www.who.int/en/news-room/fact-sheets/detail/immunization-coverage.

[27] Share the Facts. http://www.sharethefacts.org/, 2019.

[28] The commitments of the code of principals. https://ifcncodeofprinciples.poynter.org/know-more/the-commitments-of-the-code-of-principles, 2019.

[29] Bill Adair, Chengkai Li, Jun Yang, and Cong Yu. Progress toward "the holy grail": The continued quest to automate fact-checking. In *Proceedings of the 2017 Computation+Journalism Symposium*, 2017.

[30] Bill Adair, Chengkai Li, Jun Yang, and Cong Yu. Automated pop-up fact-checking: Challenges & progress. In *Proceedings of the 2019 Computation+Journalism Symposium*, 2019.

[31] Bill Adair, Mark Stencel, Cathy Clabby, and Chengkai Li. The human touch in automated fact-checking. In *Proceedings of the 2019 Computation+Journalism Symposium*, 2019.

[32] Sibel Adalı. *Modeling Trust Context in Networks*. Springer Briefs, 2013.

[33] Farahnaz Akrami, Lingbing Guo, Wei Hu, and Chengkai Li. Re-evaluating embedding-based knowledge graph completion methods. *Proceedings of the 27th ACM International Conference on Information and Knowledge Management (CIKM)*, pages 1779–1782, 2018.

[34] Y. M. Alatawi and R. A. Hansen. Empirical estimation of under-reporting in the u.s. food and drug administration adverse event reporting system (faers). *Expert Opin Drug Saf*, 16(7):761–767, 2017.

[35] M. Almukaynizi, E. Nunes, K. Dharaiya, M. Senguttuvan, J. Shakarian, and P. Shakarian. Proactive identification of exploits in the wild through vulnerability mentions online. In *2017 International Conference on Cyber Conflict (CyCon U.S.)*, pages 82–88, Nov 2017.

[36] Marcelo Arenas, Leopoldo Bertossi, and Jan Chomicki. Consistent query answers in inconsistent databases. In *PODS*, 1999.

[37] Fatma Arslan, Damian Jimenez, Josue Caraballo, Gensheng Zhang, and Chengkai Li. Modeling factual claims by frames. In *Proceedings of the 2019 Computation+Journalism Symposium*, 2019.

[38] Collin F. Baker, Charles J. Fillmore, and John B. Lowe. The berkeley framenet project. In *Proceedings of the 36th Annual Meeting of the Association for Computational Linguistics and 17th International Conference on Computational Linguistics - Volume 1*, pages 86–90, 1998.

[39] N. Ben-Asher, J.-H. Cho, and Sibel Adalı. Adaptive situational leadership framework. In *IEEE International Conference on Cognitive and Computational Aspects of Situation Management* **Best paper award**, 2018.

[40] Yoshua Bengio, Réjean Ducharme, Pascal Vincent, and Christian Jauvin. A neural probabilistic language model. *Journal of machine learning research*, 3(Feb):1137–1155, 2003.

[41] Alessandro Bessi, Fabiana Zollo, Michela Del Vicario, Antonio Scala, Guido Caldarelli, and Walter Quattrociocchi. Trend of Narratives in the Age of Misinformation. *PLoS ONE*, 10(8):e0134641–16, August 2015.

[42] Shreyas Bharadwaj, Laura Chiticariu, Marina Danilevsky, Samarth Dhingra, Samved Divekar, Arnaldo Carreno-Fuentes, Himanshu Gupta, Nitin Gupta, S-D Han, M Hernández, et al. Creation and interaction with large-scale domain-specific knowledge bases. *Proceedings of the VLDB Endowment*, 10(12):1965–1968, 2017.

[43] Antoine Bordes, Nicolas Usunier, Alberto Garcia-Duran, Jason Weston, and Oksana Yakhnenko. Translating embeddings for modeling multi-relational data. In *NIPS*, 2013.

[44] Emma E Buchtel and Ara Norenzayan. Which should you use, intuition or logic? cultural differences in injunctive norms about reasoning. *Asian Journal of Social Psychology*, 11(4):264–273, 2008.

[45] Emma E. BUCHTEL and Ara Norenzayan. Thinking across cultures: Implications for dual processes. *Oxford University Press*, 2009.

[46] Benjamin L. Bullough, Anna K. Yanchenko, Christopher L. Smith, and Joseph R. Zipkin. Predicting exploitation of disclosed software vulnerabilities using open-source data. In *Proceedings of the 3rd ACM on International Workshop on Security And Privacy Analytics*, IWSPA '17, pages 45–53, New York, NY, USA, 2017. ACM.

[47] K. Chan, J.-H. Cho, and Sibel Adalı. A trust-based framework for information sharing behavior in command and control environments. In *Proceedings of the 22nd Annual Conference on Behavior Representation in Modeling Simulation* **Best paper award**, 2013.

[48] Yi Chen, Luyi Xing, Yue Qin, Xiaojing Liao, XiaoFeng Wang, Kai Chen, and Wei Zou. Devils in the guidance: Predicting logic vulnerabilities in payment syndication services through automated documentation analysis. In *28th USENIX Security Symposium (USENIX Security 19)*, 2019.

[49] J.-H. Cho, T. Cook, S. Rager, J. O'Donovan, and Sibel Adalı. Modeling and analysis of uncertainty-based false information propagation in social networks. In *IEEE Globecom* **Best paper award**, 2017.

[50] Jin-Hee Cho, Kevin Chan, and Sibel Adali. *ACM Computing Surveys (CSUR)*, 48(2), 2015.

[51] Sutanay Choudhury, Sumit Purohit, Peng Lin, Yinghui Wu, Lawrence B. Holder, and Khushbu Agarwal. Percolator: Scalable pattern discovery in dynamic graphs. In *WSDM*, 2018.

[52] Xu Chu, Ihab F Ilyas, and Paolo Papotti. Holistic data cleaning: Putting violations into context. In *ICDE*, 2013.

[53] Michele Dallachiesa, Amr Ebaid, Ahmed Eldawy, Ahmed Elmagarmid, Ihab F Ilyas, Mourad Ouzzani, and Nan Tang. Nadeef: a commodity data cleaning system. In *SIGMOD*, 2013.

[54] Michela Del Vicario, Alessandro Bessi, Fabiana Zollo, Fabio Petroni, Antonio Scala, Guido Caldarelli, H Eugene Stanley, and Walter Quattrociocchi. The spreading of misinformation online. *Proceedings of the National Academy of Sciences*, 113(3):554–559, 2016.

[55] Berkeley J Dietvorst, Joseph P Simmons, and Cade Massey. Overcoming algorithm aversion: People will use imperfect algorithms if they can (even slightly) modify them. *Management Science*, 2016.

[56] Laura Eggertson. Lancet retracts 12-year-old article linking autism to mmr vaccines. *Lancet*, 182(4), 2010.

[57] V. A. Entwistle, S. M. Carter, A. Cribb, and K. McCaffery. Supporting patient autonomy: the importance of clinician-patient relationships. *J Gen Intern Med*, 25(7):741–5, 2010.

[58] P. Ernst, A. Siu, and G. Weikum. Knowlife: a versatile approach for constructing a large knowledge graph for biomedical sciences. *BMC Bioinformatics*, 16:157, 2015.

[59] Wenfei Fan, Yinghui Wu, and Jingbo Xu. Functional dependencies for graphs. In *SIGMOD*, 2016.

[60] Wenfei Fan, Jingbo Xu, Yinghui Wu, Wenyuan Yu, and Jiaxin Jiang. GRAPE: parallelizing sequential graph computations. *PVLDB*, 10(12):1889–1892, 2017.

[61] Wenfei Fan, Jingbo Xu, Yinghui Wu, Wenyuan Yu, Jiaxin Jiang, Zeyu Zheng, Bohan Zhang, Yang Cao, and Chao Tian. Parallelizing sequential graph computations. In *SIGMOD*, 2017.

[62] Xuan Feng, Xiaojing Liao, XiaoFeng Wang, Haining Wang, Qiang Li, Kai Yang, Hongsong Zhu, and Limin Sun. Understanding and securing device vulnerabilities through automated bug report analysis. In *28th USENIX Security Symposium (USENIX Security 19)*, 2019.

[63] Susan T Fiske and Shelley E Taylor. *Social cognition: From brains to culture*. Sage, 2013.

[64] DJ Flynn, Brendan Nyhan, and Jason Reifler. The nature and origins of misperceptions: Understanding false and unsupported beliefs about politics. *Political Psychology*, 38:127–150, 2017.

[65] Center for Behavioral Health Statistics and Quality. Results from the 2017 national survey on drug use and health: Detailed tables. Report, 2018.

[66] Xinbo Gao, Bing Xiao, Dacheng Tao, and Xuelong Li. A survey of graph edit distance. *Pattern Analysis and applications*, 13(1):113–129, 2010.

[67] Matt Gardner and Tom M Mitchell. Efficient and expressive knowledge base completion using subgraph feature extraction. In *EMNLP*, 2015.

[68] Herbert Paul Grice. Logic and conversation. In Paul Grice, editor, *Studies in the Way of Words*, pages 41–58. Harvard University Press, 1967.

[69] Big Dats Interagency Working Group. Open knowledge network: Summary of the big data IWG workshop of october 2017. 2018.

[70] C Dominik Guess. Decision making in individualistic and collectivistic cultures. *Online readings in psychology and culture*, 4(1):3, 2004.

[71] C Dominik Güss and Dietrich Dörner. Cultural differences in dynamic decision-making strategies in a non-linear, time-delayed task. *Cognitive Systems Research*, 12(3-4):365–376, 2011.

[72] Shuang Hao, Nan Tang, Guoliang Li, Jian He, Na Ta, and Jianhua Feng. A novel cost-based model for data repairing. *TKDE*, 29(4):727–742, 2017.

[73] Naeemul Hassan, Bill Adair, James T. Hamilton, Chengkai Li, Mark Tremayne, Jun Yang, and Cong Yu. The quest to automate fact-checking. In *Proceedings of the 2015 Computation+Journalism Symposium*, 2015.

[74] Naeemul Hassan, Fatma Arslan, Chengkai Li, and Mark Tremayne. Toward automated fact-checking: Detecting check-worthy factual claims by ClaimBuster. In *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, pages 1803–1812, 2017.

[75] Naeemul Hassan, Chengkai Li, and Mark Tremayne. Detecting check-worthy factual claims in presidential debates. In *Proceedings of the 24th ACM conference on Information and knowledge management (CIKM)*, pages 1835–1838, 2015.

[76] Naeemul Hassan, Afroza Sultana, You Wu, Gensheng Zhang, Chengkai Li, Jun Yang, and Cong Yu. Data in, fact out: Automated monitoring of facts by FactWatcher. *Proceedings of the VLDB Endowment (PVLDB), demonstration description*, 7(13):1557–1560, 2014. (excellent demonstration award).

[77] Naeemul Hassan, Mark Tremayne, Fatma Arslan, and Chengkai Li. Comparing automated factual claim detection against judgments of journalism organizations. In *Proceedings of the 2016 Computation+Journalism Symposium*, 2016.

[78] Naeemul Hassan, Gensheng Zhang, Fatma Arslan, Josue Caraballo, Damian Jimenez, Siddhant Gawsane, Shohedul Hasan, Minumol Joseph, Aaditya Kulkarni, Anil Kumar Nayak, Vikas Sable, Chengkai Li, and Mark Tremayne. ClaimBuster: The first-ever end-to-end fact-checking system. *Proceedings of the VLDB Endowment (PVLDB), demonstration description*, 10(12):1945–1948, August 2017.

[79] Joseph Henrich, Steven J Heine, and Ara Norenzayan. The weirdest people in the world? *Behavioral and brain sciences*, 33(2-3):61–83, 2010.

[80] Geert Hofstede, Gert Jan Hofstede, and Michael Minkov. Cultures and organizations, software of the mind. intercultural cooperation and its importance for survival. 2010.

[81] Benjamin D Horne, Sara Khedr, and Sibel Adalı. Sampling the news producers: A large news and feature data set for the study of the complex media landscape. In *ICWSM*, 2018.

[82] Benjamin D Horne, Dorit Nevo, John O'Donovan, Jin-Hee Cho, and Sibel Adali. Rating reliability and bias in news articles: Does ai assistance help everyone? 2019.

[83] Pili Hu and Wing Cheong Lau. A survey and taxonomy of graph sampling. *arXiv preprint arXiv:1308.5865*, 2013.

[84] Xiao Jiang, Chengkai Li, Ping Luo, Min Wang, and Yong Yu. Prominent streak discovery in sequence data. In *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD)*, pages 1280–1288, 2011.

[85] Damian Jimenez and Chengkai Li. An empirical study on identifying sentences with salient factual statements. In *Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN)*, pages 1–8, 2018.

[86] René F Kizilcec. How much information?: Effects of transparency on trust in an algorithmic interface. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 2390–2395. ACM, 2016.

[87] Deguang Kong, Lei Cen, and Hongxia Jin. Autoreb: Automatically understanding the review-to-behavior fidelity in android applications. In *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, pages 530–541, New York, NY, USA, 2015. ACM.

[88] Vivian Lai and Chenhao Tan. On human predictions with explanations and predictions of machine learning models: A case study on deception detection. 2019.

[89] Yeonjoon Lee, Xueqiang Wang, Kwangwuk Lee, Xiaojing Liao, XiaoFeng Wang, Tongxin Li, and Xianghang Mi. Understanding ios-based crowdturfing through hidden ui analysis. In *28th USENIX Security Symposium (USENIX Security 19)*, 2019.

[90] Timothy R. Levine. Truth-default theory (tdt): A theory of human deception and deception detection. *Journal of Language and Social Psychology*, 33(4):378–392, 2014.

[91] Stephan Lewandowsky, Ullrich KH Ecker, Colleen M Seifert, Norbert Schwarz, and John Cook. Misinformation and its correction: Continued influence and successful debiasing. *Psychological Science in the Public Interest*, 13(3), 2012.

[92] Xiaojing Liao, Kan Yuan, XiaoFeng Wang, Zhou Li, Luyi Xing, and Raheem Beyah. Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence. In *Proceedings of CCS'16*.

[93] Peng Lin, Qi Song, Jialiang Shen, and Yinghui Wu. Discovering graph patterns for fact checking in knowledge graphs. In *DASFAA*, 2018.

[94] Peng Lin, Qi Song, and Yinghui Wu. Discovering patterns for fact checking in knowledge graphs. *JDIQ*, 2019.

[95] Jenny Lindberg, Mats Johansson, and Linus Broström. Temporising and respect for patient self-determination. *Journal of medical ethics*, 45(3):161–167, 2019.

[96] Walter Lippmann. *The basic problem of democracy*. Atlantic Monthly Press, 1919.

[97] Sarthak Majithia, Fatma Arslan, Sumeet Lubal, Damian Jimenez, Priyank Arora, Josue Caraballo, and Chengkai Li. ClaimPortal: Integrated monitoring, searching, checking, and analytics of factual claims on twitter. 2019.

[98] N. E. McDonald. Vaccine hesitancy: Definition, scope and determinants. *Vaccine*, 33(34):4161–4164, 2015.

[99] Miller McPherson, Lynn Smith-Lovin, and James M Cook. Birds of a feather: Homophily in social networks. *Annual review of sociology*, 27(1):415–444, 2001.

[100] Miriam J. Metzger, Andrew J. Flanagin, and Ryan B. Medders. Social and heuristic approaches to credibility evaluation online. *Journal of Communication*, 60(3):413–439, 2010.

[101] Xianghang Mi, Ying Liu, Xuan Feng, Xiaojing Liao, Baojun Liu, XiaoFeng Wang, Feng Qian, Zhou Li, Sumayah Alrwais, and Limin Sun. Resident evil: Understanding residential ip proxy as a dark service. In *in Proceeding of the 38th IEEE Symposium on Security and Privacy*, 2019.

[102] A. M. Midboe, J. Wu, T. Erhardt, J. M. Carmichael, M. Bounthavong, M. L. D. Christopher, and R. C. Gale. Academic detailing to improve opioid safety: Implementation lessons from a qualitative evaluation. *Pain Med*, 19(suppl_1):S46–S53, 2018.

[103] Tomas Mikolov, Kai Chen, Greg Corrado, and Jeffrey Dean. Efficient estimation of word representations in vector space. *arXiv preprint arXiv:1301.3781*, 2013.

[104] Tomas Mikolov, Ilya Sutskever, Kai Chen, Greg S Corrado, and Jeff Dean. Distributed representations of words and phrases and their compositionality. In *Advances in neural information processing systems*, pages 3111–3119, 2013.

[105] Frank Luther Mott. *American Journalism 1690-1940*, volume 4. Psychology Press, 2000.

[106] Mohammad Hossein Namaki, F. A. Rezaur Rahman Chowdhury, Md Rakibul Islam, Janardhan Rao Doppa, and Yinghui Wu. Learning to speed up query planning in graph databases. In *ICAPS*. AAAI, 2017.

[107] Mohammad Hossein Namaki, Peng Lin, and Yinghui Wu. Event pattern discovery by keywords in graph streams. In *BigData*. IEEE, 2017.

[108] Mohammad Hossein Namaki, Keyvan Sasani, Yinghui Wu, and Tingjian Ge. Beams: bounded event detection in graph streams. In *Data Engineering (ICDE), 2017 IEEE 33rd International Conference on*, 2017.

[109] Mohammad Hossein Namaki, Keyvan Sasani, Yinghui Wu, and Tingjian Ge. BEAMS: bounded event detection in graph streams. In *ICDE*, 2017.

[110] Mohammad Hossein Namaki, Yinghui Wu, Qi Song, Peng Lin, and Tingjian Ge. Discovering graph temporal association rules. In *CIKM*, 2017.

[111] Mohammad Hossein Namaki, Yinghui Wu, and Xin Zhang. Gexp: Cost-aware graph exploration with keywords. In *SIGMOD*, 2018.

[112] Maximilian Nickel, Kevin Murphy, Volker Tresp, and Evgeniy Gabrilovich. A review of relational machine learning for knowledge graphs. *Proceedings of the IEEE*, 104(1):11–33, 2016.

[113] Richard Nisbett. *The geography of thought: How Asians and Westerners think differently... and why*. Simon and Schuster, 2004.

[114] Jeppe Norregaard, Benjamin D Horne, and Sibel Adali. Nela-gt-2018: A large multi-labelled news dataset for the study of misinformation in news articles. 2019.

[115] Petra Kralj Novak, Nada Lavrač, and Geoffrey I Webb. Supervised descriptive rule discovery: A unifying survey of contrast set, emerging pattern and subgroup mining. *Journal of Machine Learning Research*, 10(Feb):377–403, 2009.

[116] Brendan Nyhan and Jason Reifler. When corrections fail: The persistence of political misperceptions. *Political Behavior*, 32(2):303–330, 2010.

[117] Leo Obrst, Penny Chase, and Richard Markeloff. Developing an ontology of the cyber security domain. In *STIDS*, pages 49–56, 2012.

[118] E. Pariser. *The Filter Bubble: What The Internet Is Hiding From You*. Penguin Books Limited, 2011.

[119] Heiko Paulheim. Knowledge graph refinement: A survey of approaches and evaluation methods. *Semantic web*, 8(3):489–508, 2017.

[120] Gordon Pennycook and David G. Rand. Who falls for fake news? the roles of bullshit receptivity, overclaiming, familiarity, and analytic thinking. *Journal of Personality*, March 2019.

[121] R. E. Petty and J. T Cacioppo. The elaboration likelihood model of persuasion. In *In Communication and Persuasion*, pages 1–24. New York: Springer, 1986.

[122] PSNet. Medication errors and adverse drug events. Report, Agency for Healthcare Research and Quality, 2019.

[123] D. M. Qato, G. C. Alexander, R. M. Conti, M. Johnson, P. Schumm, and S. T. Lindau. Use of prescription and over-the-counter medications and dietary supplements among older adults in the united states. *JAMA*, 300(24):2867–78, 2008.

[124] Yinghui Wu Qi Song, Mohammad Hossein Namaki. Answering why-questions for subgraph queries in multi-attributed graphs. In *ICDE*, 2019.

[125] Yi Qian and Sibel Adalı. Foundations of trust and distrust in networks: Extended structural balance theory. *ACM Transactions on the Web (TWEB)*, 8(3):13:1–13:33, 2014.

[126] Emilee Rader, Kelley Cotter, and Janghee Cho. Explanations as mechanisms for supporting algorithmic transparency. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, page 103. ACM, 2018.

[127] Recorded Future. Recorded Future at SITA. https://go.recordedfuture.com/hs-fs/hub/252628/file-2607572540-pdf/case-studies/sita.pdf, 2015.

[128] Website repository for incentive-based truth elicitation crowdsourcing system. https://sites.google.com/site/reportingtruthful/.

[129] Rob McMillan. Open Threat Intelligence. https://www.gartner.com/doc/2487216/definition-threat-intelligence, 2013.

[130] Carl Sabottke, Octavian Suciu, and Tudor Dumitra. Vulnerability disclosure in the age of social media: exploiting twitter for predicting real-world exploits. In *24th {USENIX} Security Symposium ({USENIX} Security 15)*, pages 1041–1056, 2015.

[131] A. Sapienza, A. Bessi, S. Damodaran, P. Shakarian, K. Lerman, and E. Ferrara. Early warnings of cyber threats in online discussions. In *2017 IEEE International Conference on Data Mining Workshops (ICDMW)*, pages 667–674, Nov 2017.

[132] Keyvan Sasani, Mohammad Hossein Namaki, Yinghui Wu, and Assefaw Hadish Gebremedhin. Multi-metric graph query performance prediction. In *DASFAA*, 2018.

[133] P. R. Shankar. Vigiaccess: Promoting public access to vigibase. *Indian J Pharmacol*, 48(5):606–607, 2016.

[134] S. Sikdar, B. Kang, J. O'Donovan, T. Hollerer, and S. Adalı. Understanding information credibility on twitter. In *International Conference on Social Computing (SocialCom)* **Best paper award**, 2013.

[135] T.C. Smith. Vaccine rejection and hesitancy: A review and call to action. *Open Forum Infectious Diseases*, 4(3), 2017.

[136] Verizon Enterprise Solutions. Data breach investigations report. *MC15912*, 4:14, 2014.

[137] Qi Song, Bo Zong, Yinghui Wu, Lu An Tang, Hui Zhang, Guofei Jiang, and Haifeng Chen. Tgnet: Learning to rank nodes in temporal graphs. In *CIKM*, 2018.

[138] Shaoxu Song, Boge Liu, Hong Cheng, Jeffrey Xu Yu, and Lei Chen. Graph repairing under neighborhood constraints. *The VLDB Journal*, 26(5):611–635, 2017.

[139] F. S. Spear, B. Hallett, Sibel Adalı J. M. Pyle, B. K. Szymanski, A. Waters, Z. Linder, S. O. Pearce, M. Fyffe, D. Goldfarb, N. Glickenhouse, and H. Buletti. Metpetdb: A database for metamorphic geochemistry. *Geochem. Geophys. Geosyst.*, 10(12):Q12005, 2009.

[140] Afroza Sultana, Naeemul Hassan, Chengkai Li, Jun Yang, and Cong Yu. Incremental discovery of prominent situational facts. In *Proceedings of the 30th International Conference on Data Engineering(ICDE)*, pages 112–123, 2014.

[141] Charles S Taber and Milton Lodge. Motivated skepticism in the evaluation of political beliefs. *American Journal of Political Science*, 50(3):755–769, 2006.

[142] Zijing Tan and Liyong Zhang. Improving xml data quality with functional dependencies. In *DASFAA*, 2011.

[143] Brett Walenz, Junyang Gao, Emre Sonmez, Yubo Tian, Yuhao Wen, Charles Xu, Bill Adair, and Jun Yang. Fact checking congressional voting claims. In *Proceedings of the 2016 Computation+Journalism Symposium*.

[144] Brett Walenz, You (Will) Wu, Seokhyun (Alex) Song, Emre Sonmez, Eric Wu, Kevin Wu, Pankaj K. Agarwal, Jun Yang, Naeemul Hassan, Afroza Sultana, Gensheng Zhang, Chengkai Li, and Cong Yu. Finding, monitoring, and checking claims computationally based on structured data. In *Proceedings of the 2014 Computation+Journalism Symposium*, 2014.

[145] Brett Walenz and Jun Yang. Perturbation analysis of database queries. *Proceedings of the VLDB Endowment*, 9(14), 2016.

[146] Peng Wang, Xianghang Mi, Xiaojing Liao, XiaoFeng Wang, Kan Yuan, Feng Qian, and Raheem Beyah. Game of missuggestions: Semantic analysis of search-autocomplete manipulations. In *in the proceeding of ISOC Network and Distributed System Security Symposium*, 2018.

[147] Qi Wang. Why should we all be cultural psychologists? lessons from the study of social cognition. *Perspectives on Psychological Science*, 11(5):583–596, 2016.

[148] Quan Wang, Jing Liu, Yuanfei Luo, Bin Wang, and Chin-Yew Lin. Knowledge base completion via coupled path ranking. In *ACL*, 2016.

[149] P. C. Webster. Oxycodone class action lawsuit filed. *CMAJ*, 184(7):E345–6, 2012.

[150] You Wu, Pankaj K. Agarwal, Chengkai Li, Jun Yang, and Cong Yu. On "one of the few" objects. In *Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD)*, pages 1487–1495, 2012.

[151] You Wu, Pankaj K. Agarwal, Chengkai Li, Jun Yang, and Cong Yu. Toward computational fact-checking. In *Proceedings of the VLDB Endowment (PVLDB)*, volume 7, pages 589–600, 2014.

[152] You Wu, Pankaj K. Agarwal, Chengkai Li, Jun Yang, and Cong Yu. Computational fact checking through query perturbations. *ACM Transactions on Database Systems (TODS)*, 42(1):4:1–4:41, 2017.

[153] You Wu, Brett Walenz, Peggy Li, Andrew Shim, Emre Sonmez, Pankaj K. Agarwal, Chengkai Li, Jun Yang, and Cong Yu. iCheck: Computationally combating "lies, d–ned lies, and statistics". In *Proceedings of the 2014 ACM SIGMOD International Conference on Management of Data (SIGMOD), demonstration description*, pages 1063–1066, 2014.

[154] Zonghan Wu, Shirui Pan, Fengwen Chen, Guodong Long, Chengqi Zhang, and Philip S Yu. A comprehensive survey on graph neural networks. *arXiv preprint arXiv:1901.00596*, 2019.

[155] Mingyan Xiao, Wenqiang Jin, Ming Li, and Chengkai Li. Eliciting joint truthful data and cost from strategic participants in crowdsourcing systems. In *Under submission*, 2019.

[156] Yinghui Wu XUanming Liu, Tingjian Ge. Finding densest lasting subgraphs in dynamic graphs: a stochastic approach. In *ICDE*, 2019.

[157] Ning Yan, Sona Hasani, Abolfazl Asudeh, and Chengkai Li. Generating preview tables for entity graphs. In *Proceedings of the 2016 ACM SIGMOD International Conference on Management of Data (SIGMOD)*, pages 1797–1811, 2016.

[158] Jun Yang, Pankaj K. Agarwal, Sudeepa Roy, Brett Walenz, You Wu, Cong Yu, and Chengkai Li. Query perturbation analysis: An adventure of database researchers in fact-checking. *IEEE Data Eng. Bull.*, 41(3):28–42, 2018.

[159] Kan Yuan, Haoran Lu, Xiaojing Liao, and XiaoFeng Wang. Reading thieves' cant: Automatically identifying and understanding dark jargons from cybercrime marketplaces. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 1027–1041, Baltimore, MD, 2018.

[160] Gensheng Zhang, Xiao Jiang, Ping Luo, Min Wang, and Chengkai Li. Discovering general prominent streaks in sequence data. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 8(2):9:1–9:37, June 2014.

[161] Gensheng Zhang, Damian Jimenez, and Chengkai Li. Maverick: Discovering exceptional facts from knowledge graphs. In *Proceedings of the 2018 ACM SIGMOD International Conference on Management of Data (SIGMOD)*, pages 1317–1332, 2018.

[162] Gensheng Zhang and Chengkai Li. Maverick: A system for discovering exceptional facts from knowledge graphs. *Proceedings of the VLDB Endowment (PVLDB), demonstration description*, 11(12):1934–1937, August 2018.

[163] C. Zheng and R. Xu. Large-scale mining disease comorbidity relationships from post-market drug adverse events surveillance data. *BMC Bioinformatics*, 19(Suppl 17):500, 2018.

[164] Rong Zhou and Eric A Hansen. Beam-stack search: Integrating backtracking with beam search. In *ICAPS*, pages 90–98, 2005.

List of Project Personnel and Partner Institutions

Name	Role	Affiliation
Chengkai Li	PI	The University of Texas at Arlington
Sibel Adali	Co-PI	Rensselaer Polytechnic Institute
Xiaojing Liao	Co-PI	Indiana University
Yinghui Wu	Co-PI	Washington State University
Jun Yang	Co-PI	Duke University
Gautam Das	Senior Personnel	The University of Texas at Arlington
Ming Li	Senior Personnel	The University of Texas at Arlington
Shirin Nilizadeh	Senior Personnel	The University of Texas at Arlington
Mark Tremayne	Senior Personnel	The University of Texas at Arlington
Yan Xiao	Senior Personnel	The University of Texas at Arlington
Jie Jennifer Zhang	Senior Personnel	The University of Texas at Arlington
Lavanya Vasudevan	Paid Consultant	Duke University
Juliana Freire	Subawardee	New York University
Naeemul Hassan	Subawardee	The University of Maryland, College Park
Daniel Krawczyk	Subawardee	The University of Texas at Dallas
Ashwin Machanavajjhala	Subawardee	Duke University
Miriam Metzger	Subawardee	University of California - Santa Barbara
Lauren Santoro	Subawardee	The University of Texas at Dallas
Jonathan Bakdash	Unpaid Consultant	United States Army Research Laboratory
Sutanay Choudhury	Unpaid Consultant	Pacific Northwest National Laboratory
Giovanni da San Martino	Unpaid Consultant	Qatar Computing Research Institute
Marina Danilevsky	Unpaid Consultant	IBM Research - Almaden
Xin Luna Dong	Unpaid Consultant	Amazon
Jing Gong	Unpaid Consultant	Temple University
Yunyao Li	Unpaid Consultant	IBM Research - Almaden
Laura Marusich-Cooper	Unpaid Consultant	United States Army Research Laboratory
Preslav Nakov	Unpaid Consultant	Qatar Computing Research Institute
Alun Preece	Unpaid Consultant	Cardiff University, U.K.
Char Sample	Unpaid Consultant	ICF International, Inc.
Nan Tang	Unpaid Consultant	Qatar Computing Research Institute
Cong Yu	Unpaid Consultant	Google Research