Towards A Biometric Authentication-based Hybrid Trust-computing Approach for Verification of Provider Profiles in Online Healthcare Information

Ankur Chattopadhyay, Michael J. Schulz, Clinton Rettler, Katie Turkiewicz, Laleah Fernandez and Askar Ziganshin
Department of Information and Computing Sciences
University of Wisconsin - Green Bay
Green Bay, USA

Abstract - **With the advent of the Internet and the growth in the use of cyberspace by consumers for online healthcare information (OHI), various researchers from different disciplines have been working on the challenges and threats posed by the issue of cyberchondria, which is related to the cyber psychological aspects of uncertainty, anxiety, quality, and credibility. However, there are few research efforts, which have directly treated the case of cyberchondria as an interdisciplinary trust-computing problem in information assurance. None of these efforts has encountered the reliability issues with OHI, leading to cyberchondria, by handling provider level trust antecedents. OHI based trust research has also never used biometrics to validate multi-dimensional trust constructs, including visual appearance, reputation, familiarity and social identity. Additionally, this research avenue has not handled the trustworthiness of OHI at the provider level through verification of institutional profiles and affiliations. Hence, in order to enhance trustworthiness through verification at the trustee level, this paper conceptualizes and proposes a novel trust-computing model, which is driven by visual recognition based biometric authentication of physician profiles. The uniqueness of this hybrid trust model lies in its biometric-inspired basis and provider-centric approach, along with its fine blend of soft trust and hard trust elements. As an initial proof-of-concept prototype for the proposed approach, an experiment is conducted to demonstrate a potential implementation of this trust-computing model. The experimental results obtained through this prototype implementation are shared as part of this paper. This prototype will drive further innovative experiments with the proposed trust-computing model, and shall form the basis of future trust related research in OHI for addressing cyberchondria.**

Keywords – antecedents; authentication; biometric; consumer; cyberchondria; hard trust; hybrid trust; online healthcare information; provider; soft trust; visual recognition; verification

I. INTRODUCTION

The Internet profoundly impacts the way people search for, utilize, and communicate about healthcare information. According to a nationwide survey on Internet use, eight out of ten American adults search online for healthcare information [1]. More specifically, 83% of those surveyed indicated using the Internet to look up a particular disease or medical problem [11]. In short, there is a tremendous amount of OHI available to the typical consumer and there are no standard mechanisms and regulations, including credibility standards for OHI, that embodies or characterizes how to make 'trust' decisions as online healthcare consumers [37]. Although active OHI users make such 'trust' judgments all the time, there is no method or approach to comply with the rationale of making such decisions [40].

The topic of online information trust is a particularly important issue in the context of health information acquisition. While record numbers of U.S. adults are turning to the Internet to self-diagnose, seek treatment options and choose a physician, many people encounter a number of challenges. The inability to find accurate information [2], inconsistent advice or information [10, 24], the inability to make sense of health information [3] and the psychological distress resulting from the information seeking process [4] are all examples of some of these challenges. For example, cyberchondria is the experience of heightened anxiety related to medical disorders resulting from online health information seeking [5]. Research in this field suggests that some people are particularly vulnerable to bouts of distress related to online information seeking. Individuals with high health anxiety seek online health information more frequently and spend longer searching online. Individuals with high health anxiety find searching for health information online more distressing and anxiety provoking. At the same time, levels of health anxiety are positively related to the frequency and the duration of online health information searches [6]. This cyclical pattern of distress in information seeking have detrimental effects on the individual, who is generally already suffering from an acute or chronic health condition that prompted the initial search.

The notion of trust can be attributed to a multi-dimensional, multi-disciplinary concept with a complex interpersonal connotation and social context [11, 12, 14, 20, 23, 37]. However, the OHI seeking and cyberchondria related trust issues have never been researched from the perspective of soft trust and hard trust components [40] as applicable in computing disciplines [27, 34]. One important component of trust has to do with user rejection or selection of a particular site, it stands to reason that consumers will engage with sites they view as trustworthy and reject those they mistrust [10, 24]. Research in the area of online health information trusts suggest *mistrust* of websites is based on design factors, including the use of images [3] while *trust* of websites is based on content factors such as source credibility and

DOI 10.1109/SPW.2017.23

personalization [10, 24]. For example, [21] argues that consumers tend to trust sites with visual appeal and mistrusting those with poor visual design. Thus, images as part of the design or visual appeal can play a guiding role in user trust of online health information. This heightened trust has the potential to decrease anxiety associated with the information acquisition process.

A number of studies have noted a link between the use of images and user trust of health websites. These studies suggest that images increase trust by creating a sense of familiarity or endorsement. Consumers appear to be influenced by the branding of the site or by the presence of familiar images or trusted logos [10, 21, 24]. For example, [2] found that online design factors such as visual appeal, first impression, images and video messages on the web worked as lure among elderly adults seeking online health information thereby creating a personal connection between the user and the content. Existing literature [10, 19, 21, 22, 24, 36] argue that trust in OHI can be influenced by trust inducing attributes like website endorsements, scientific imagery and prominent features, such as photographs. They suggest that the quality of information available on a website plays a role along with the perceived profile plus expertise of the providers (or the physicians). They also reason that OHI trust is driven by the extent to which the provider appears to be familiar and connectable through a shared social identity.

A. The Cyberchondria Connection: Issues and Challenges

Cyberchondria has been considered as a distinct mental disorder and a multidimensional concept with mistrust of medical professionals as one of its key features [7]. Cyberchondria is not simply hypochondriacs using the Internet, but rather a distinct form of online information seeking and resulting escalating health anxiety. Recent research has found that cyberchondria is actually more closely aligned with other forms of problematic Internet use (i.e., compulsive online shopping, online gambling, and online pornography consumption) than traditional hypochondria [4].

More specifically, behavioral manifestations of hypochondria and cyberchondria are where the key differences between the two become apparent. Cyberchondria involves a cerebral response to a lack of information. Conversely, hypochondriacs convince themselves they are suffering from a specific medical condition, manifest physical reactions to their perceived symptoms, and engage in behaviors that enact their concerns (i.e., going to see a doctor). Therefore, the enactment of cyberchondria is far less physical and disruptive, as it centers on increased cerebral efforts to gather information. The primary impetus for hypochondria is the conviction that one has a specific medical condition, whereas cyberchondria is primarily driven by a desire to acquire more information about a specific condition. Furthermore, cyberchondria is less likely to evolve into behavioral responses and more likely to be sustained at the cerebral level. The lower levels of physical commitment make cyberchondria more diffuse and manageable than hypochondria.

Cyberchondria has been a social phenomenon that has evolved along with the increase in Internet use for obtaining online health information i.e. with the rise in online healthcare consumerism [5]. The topic of cyberchondria provides fertile ground for social science researchers, and more specifically, for communication scholars. The impact of cyberchondria can be examined from a communicative perspective through the lens of technology scholarship, health communication, and interpersonal research [4]. One of the ways people are employing the Internet for their health care needs is as a diagnostic tool [9]. People input various search engine queries related to symptoms they may be experiencing or are interested in understanding better and view the search results as carrying some authority. This is also sometimes pejoratively referred to as “asking Dr. Google.”

The social implications of cyberchondria are substantial, but for the sake of brevity, this discussion will expand on the larger issues of online health information credibility. Any form of problematic or compulsive use of the Internet has social impact [7]. What makes cyberchondria a unique challenge is the component of personal health. A person’s physical well-being is never to be taken lightly and the ubiquity of erroneous or misleading health information on the Internet is a very real issue. This leaves the online health information seeker with the sole responsibility of wading through all the available information to determine what is credible. Consequently, there are individuals routinely seeking out health information online only to be misled or misinformed. The primary concern is a distorted or inaccurate perception of personal risk due to online misinformation and deception. The potentially erroneous information, which people find while online, can lead to unfounded anxiety [6]. Furthermore, the hope that the quality of online health information will improve over time is extremely unlikely. There are reputable and credible sources of health information online, but online health information is not regulated and should never take the place of a health care provider’s examination, treatment, or advice.

The increasing availability of health information online (whether credible or not) is not the only contributing force behind cyberchondria [9]. Another factor to be considered is the health care consumerism movement. Modern consumer culture has generated attitudes toward health care as a lifestyle choice that is personally managed and maintained. Taking an increased interest in personal health decisions is not inherently problematic, but generally considered proactive and admirable. Furthermore, people interested and involved with their own healthcare are more likely to improve their health circumstances. An unfortunate and extreme response to the health care consumerism movement has resulted in some people selectively ignoring or avoiding professional medical care and using the Internet as a major information source for their health care needs. This is leading them to information without medical guidance and supervision.

Potentially dubious online health information and health care consumerism are social impact issues contributing to cyberchondria that generally fall under individual control. The effect cyberchondria can have on the relationship and communication of a patient and a health care provider broadens the impact more directly to social interactions and relationships. The impact of cyberchondria on the health care

provider-patient relationship has been previously examined [5, 6]. The overall assessments vary from marginally positive (i.e., a patient's improved access to online healthcare information supports patient empowerment and an improved partnership with the health care provider in proactively managing personal health) to very negative (i.e., health care providers resent being questioned by their patients about healthcare decisions, feel the Internet promotes 'doctor shopping,' and sometimes take punitive measures with Internet-informed patients who question their authority). For better or worse, the availability of online health information and how people chose to consume it is fundamentally changing how patients interact with their health care providers.

The avenues of potential research into the phenomenon of cyberchondria are vast. As a form of problematic Internet use, cyberchondria can be readily examined from the perspective of technology and its impact on social change [4]. As previously discussed, the health care provider-patient communication dynamic has already been established as a dyad significantly influenced by the availability of online health information. It is important to clarify that simply going on the Internet to research a health-related topic does not make someone a cyberchondriac. Similarly, a diagnosed hypochondriac who uses the Internet to seek out health information does not become a cyberchondriac rather than a hypochondriac.

Overall, cyberchondria has evolved from a number of factors including increased Internet availability, increased Internet access, health care consumerism, and the costly health care system [7]. The current issues of vast amounts of dubious health information on the Internet, increasing demands on the healthcare system, the overall decline in national health, the increasing elderly population, and the steady rise in diagnosed chronic medical conditions ensure that the role of technology in healthcare will only expand. As people increasingly turn to technology for answers and assistance, it is vital that medical professionals and researchers fully understand the limitless potential it can have to both supplement and undermine an individual's ability to personally manage their own health.

Non-technical social sciences research disciplines (like communications, psychology) can contribute in a meaningful way to understanding how cyberchondria affects society. However, it needs to collaborate with computing disciplines for providing actual tangible solutions. This is where finding innovative application tool based solutions to determining the credibility of online health information become essential. This paper builds the foundation for future interdisciplinary research on providing technical models to determine an "antidote" to cyberchondria. The prototype implementation of the unique biometric authentication based OHI trust model, as proposed in this paper, represents the start of a much larger project anchored in OHI trust assessment. Automating the examination of healthcare provider profiles for biometric trust markers and accuracy leads to building an innovative software tool with the potential to evaluate OHI by computing trust value. This would provide users with an improved trustworthy perception of OHI, thereby mitigating the effects of cyberchondria.

B. Importance and Motivation of Research

Trust can be a mediating factor for addressing the challenges associated with OHI seeking and for countering cyberchondria, as discussed in the previous sections. Recent papers like [9] directly argue that the effects of cyberchondria can be minimized if online healthcare consumers can find an easy way of determining the trustworthiness of an OHI website. The research presented in this paper is firstly motivated by the need of persuasive imagery in building trust in OHI, as cited in the earlier section. This forms the basis of using visual profiles at the provider level for the trust-computing model proposed in this paper.

Secondly, what inspires this research work is the requirement of establishing trustworthiness in OHI, as part of information assurance, which the proposed research handles innovatively through biometric authentication. Recent literature [10, 14, 21, 37] emphasizes the development of trust in OHI through systematic evaluation of content, concluding that consumers are more likely to trust OHI if they could verify the available information by crosschecking it with other websites through integration of information across multiple sources and different sites. Even though few publications [12, 15, 37] discuss credibility and acceptability as contributing factors towards trustworthiness of online information, they do not actually illustrate or demonstrate how the process of authentication can be employed to serve the cause. In this aspect, this paper is the first of its kind to apply computer vision [27], in the form of visual recognition based biometric authentication, towards the field of OHI to innovate data evaluation via cross-verification.

It should be noted herein that there has been some ongoing research [31, 32] in ubiquitous, connected healthcare, using sensors and cloud computing for enhancing trust computing. These efforts have made use of sophisticated models of user authentication, including user reputation based profiles, and role based access control systems for improving healthcare. However, this paper focuses on a problem within the sphere of online healthcare consumerism associated with the issue of cyberchondria, which is a different and stand apart case. There also has been recently some trust, authentication and reputation based research [13, 15, 16] on web content in relation to e-commerce and social media platforms like Twitter, Facebook, etc. These efforts have looked into the user trust, confidence and credibility levels using social profiles through techniques like machine learning based classification and analysis by cross-validation based authentication and verification via trusted sources. However, none of the OHI research has directly used visual recognition based machine learning for addressing trust and reputation through a biometric authentication and verification process.

Additionally, the previous trust computing models in OHI [12, 19, 37] have employed user-centric models for evaluating trust. These models have only been limited to covering trust constructs at the consumer and website levels [18, 20]. Existing literature [11, 14, 33] argue that trust is a multi-dimensional entity and needs to be expanded to a broader context by considering trust inducing factors at the institutional level. Most OHI trust related research [23, 25, 26] has traditionally accounted for only trustor-focused attributes. They have typically undermined or neglected the

organizational trust antecedents like expert (or provider) profile, reputation, verification, familiarity and social identity [18, 20]. Some researchers clearly make the point how perceived credentials of involved experts in OHI can make an impact on building trust in OHI [14, 21, 22]. Thus, in order to fill in these mentioned gaps in OHI trust related research practice, this paper proposes a new provider-centric OHI trust computing model, which extends the determination of trustworthiness to the trustee level by validating institutional trust components like provider perception, reputation, verification, acquaintance and social connect through biometric authentication unlike other trust models.

Lastly, the OHI trust related research described in this paper analyzes the trust computing model from the perspective of soft trust and hard trust [27, 34], and this has never been done before. Therefore, this paper thrives towards conducting a soft trust and a hard trust based analysis [40] within the OHI realm for the very first time. The novelty of this paper lies in the hybrid trust approach [35] that is proposed here for improving the trust-based decision making of OHI seekers. Thereby, this research effort is to help take a positive step towards mitigating cyberchondria.

As mobile technology continues to seamlessly integrate into the modern lifestyle and the national healthcare system continues to be intractable, it is imperative to have an effective and reliable resource, in the form of a trust computing model, for determining the credibility, authenticity and acceptability of OHI. The current research, as presented here, seeks to address the above demands of the OHI trust domain and enhance the contemporary state of the art work. Overall, this paper introduces a fresh provider-centric OHI trust-computing model, that is driven by biometric authentication. Additionally, the research study conducted in this paper explores the role of trust in OHI acquisition from a unique hybrid standpoint, and proposes a technical solution to reduce the potential anxiety associated with the process of seeking accurate and relevant OHI. This proposed solution paves the path for the making of a tool to determine the credibility, authenticity and trust of OHI.

II. Integrating Soft Trust with Hard Trust

There are several OHI websites that contain healthcare service provider related details. The driving question, which that the common OHI seeker is routinely faced with [9], is which source to trust? With only the webpage content as the means for assessing trustworthiness and credibility, the importance of that content for user trust assessments is substantial. To illustrate this issue, a few different OHI websites are examined and explained. The first one, ABIM (American Board of Internal Medicines).org [30], is a well-known and medically accredited website with board certifications and professional endorsements. This website provides board certification information for the healthcare providers it features. Board certified credentials are an example of hard trust features [25, 40]. In addition to the board certifications, abim.org features physician photographic profiles that can act as visual biometric indicators that can be computed through cross-reference with other photo profiles from different online sources for verification purposes. The use of hard trust features, including biometric attributes, on ABIM.org, sets up an opportunity for comparison to other non-accredited OHI websites dominated by soft trust elements.

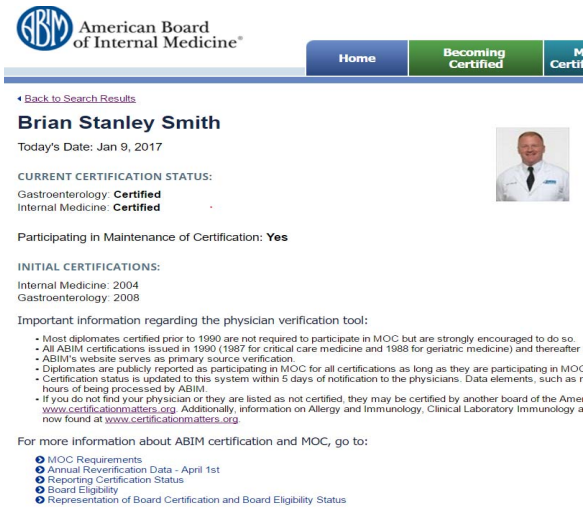

Fig. 1. ABIM.org [30] Profile of Brian Stanley Smith, MD.

HealthGrades.com [29] and ZocDoc.com [28] are both examples of websites intended for healthcare consumers seeking OHI. These sites contain data on healthcare service providers as well as reviews on physicians authored by patients. These contents play a role in formation of consumer opinions leading to user beliefs. The healthcare consumers have to determine on their own if they will trust the authenticity and accuracy of these user data as available on these websites. The contents of such OHI websites can be useful and may be regarded as valuable by public consumers, but they lack validation due to the possibility that they have been manipulated or even fabricated. If a trust decision is taken on the basis of the soft user contents of such websites, then that would lead to case of soft trust building without hard trust assessment.

Figures 1 and 2 display preview profiles of the same physician, Brian Stanley Smith, including headshot photos in ABIM.org and HealthGrades.com respectively. Similarly, Figure 3 shows the online screenshot of the visual profile of another physician, William Montesano on ZocDoc.com. According to the biometric trust-computing model, as proposed in this paper, the physician profiles in these two websites can be validated against one another using biometrics on the visual contents. In other words, the healthcare service provider based soft content hosted on common healthcare consumer-focused websites (like HealthGrades.com and ZocDoc.com) can be examined using corresponding physician profile data from medically accredited websites (like ABIM.org or the official healthcare provider website resources) using vision computing based biometric authentication.

This technical process of provider-centric cross validation using biometrics lays the foundation for a hard-trust computing mechanism using soft data and creates a hybrid trust paradigm, the first of its kind in validating OHI. This hybrid trust model is intended for developing more confidence and added credibility among OHI users. It is also meant to

provide more peace of mind to users for important trust decisions, and counter cyberchondria in the process through verification of OHI trustworthiness via biometric authentication. Combining hard and soft trust elements in the described hybrid approach to determine trustworthiness is a more comprehensive and effective indicator of credibility in OHI. This is because the proposed model, unlike other existing models, elegantly handles and validates the institutional trust antecedents beyond the usual scope of the consumer and website.

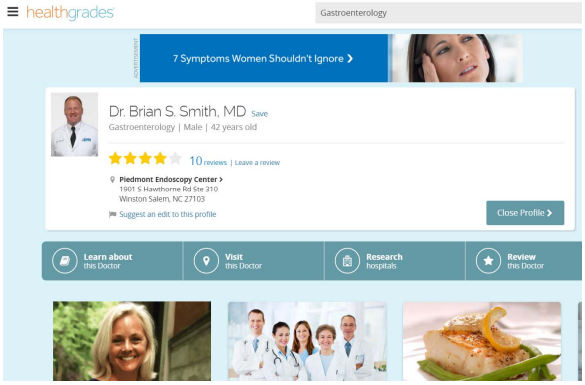

Fig. 2. HealthGrades.com [29] Profile of Brian Stanley Smith, MD.

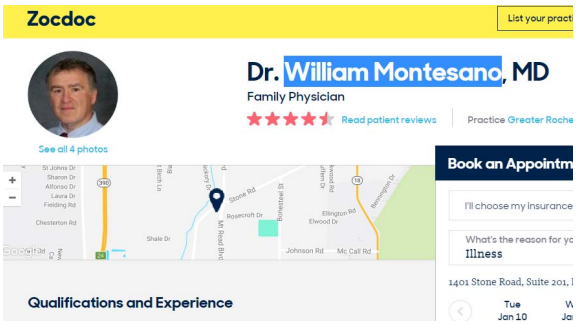

Fig. 3. ZocDoc.com [28] Profile of William J. Montesano, MD.

III. Visual Recognition Biometrics To Improve Trust

The use of biometrics in conjunction with computer vision [27] has yielded in robust authentication processes in the field of security earning user trust and assurance. Successful instances of biometrics include fingerprint scanning, retina identification, and voice recognition implemented in advanced technological applications and trusted secure facilities. However, existing literature on OHI and cyberchondria suggest that neither biometrics nor vision computing has been meaningfully applied to benefit and enhance the trust values of online healthcare consumers. There is a large number of non-recognized healthcare websites available online that lack any sort of official certification or endorsement. Yet, they publish a lot of detailed information on healthcare service providers as well as physician profiles, including photographic images on some instances. This raises a common trust issue for OHI users and poses the question as to how to validate these non-accredited online profiles.

A. *Proposed Biometric Trust Computing Model*

The proposed biometric OHI trust-building approach is modelled using a visual recognition based computing paradigm, as depicted in Figure 4. In order to implement a proof-of-concept prototype application for conducting a research experiment, IBM Watson's visual recognition platform [8] is chosen as a biometric computing platform for evaluating trust in OHI. As illustrated in Figure 5, the visual recognition application sets up an image classifier file using images acquired from accredited medical databases. The classifier is then used to analyze images acquired from the OHI websites and returns a matching score for each image. All biometric scores are subsequently recorded and tallied to provide an overall provider-centric trust indicator.

B. *Image Souces for Biometric Trust Computing Experiment*

Various physician image profiles were chosen from several different OHI websites and a recognized provider network for implementing the proposed biometric authentication model as part of the conducted research experiment. These images contributed towards the construction of the distinct image classes needed for the experiment. A mixture of both medically accredited sites and social database sites were used in order to conduct the intended research experiment. HealthGrades.com [29], American Board of Internal Medicine (ABIM) [30] and ZocDoc.com [28] were utilized to pick images for the facial recognition test as well as corresponding training associated with the image classifier. Physician images from the Aspirus online medical staff directory [38] were chosen as the primary reference for the biometric validation experiment along with Greater Rochester Internal Medicine [39] and ABIM.

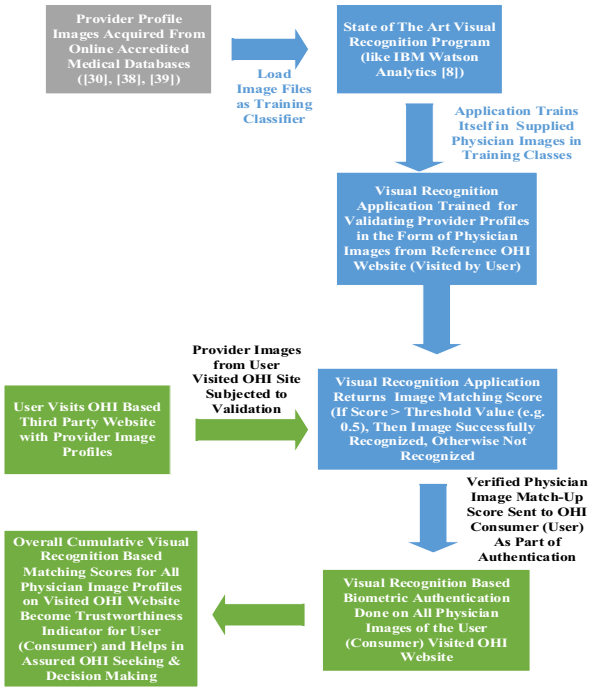

Fig. 4. Block Diagram Representing Proposed Visual Recognition Driven Biometric Trust Computing Model for Enhancing OHI Trustworthiness.

C. *Training IBM Watson for Visual Recognition*

Upon acquiring the experimental physician image profiles from the selected OHI websites, these were placed into a compressed file and submitted to IBM's Watson Developer Cloud node.js interface [8]. Images from Aspirus [38], ABIM [30], and Greater Rochester Internal Medicine [39] were divided into two different classes, each named General Practitioner and Internal Medicine corresponding to each category of physician listed on the chosen sites. This experimental set up was intended to illustrate that the biometric classification can be driven not only by facial recognition, but also by the physician's area of medical expertise as an added matching attribute. The overall algorithmic process of IBM Watson's visual recognition analytics is depicted in Figure 5.

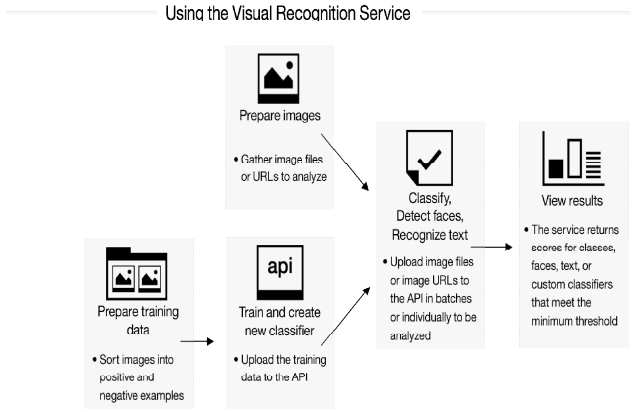

Fig. 5. Block Diagram Representing the Algorithmic Process Used by the Visual Recognition Based Analytics Service of IBM Watson [8].

D. *IBM Watson Visual Recognition Experimental Results*

Upon running the trained classifier images for validating a carefully selected sample set of 20 physician photographic profiles, seventeen of the images were recognized above IBM Watson's accepted threshold score of 0.5 for visual recognition [8]. The first set of images were obtained from HealthGrades.com [29] and cross-checked against the Aspirus database [38]. The highest score result of the entire experiment was obtained from this set of data and achieved a score of 0.60 as shown in Figure 11. As per our observations, there were significant differences in image quality between physician photo profiles taken from the Aspirus database and the HealthGrades website, as well as intra-class quality variations between physician images within the same classifier category.

It is to be noted that as a major part of the conducted experiments (as exhibited in Figures 6 to 11), the Aspirus physician profiles were used for validating the HealthGrades.com images. Another part of the practical experiment was conducted by biometrically authenticating physician photographic images taken from ZocDoc.com [28] using the photo profiles from Greater Rochester Internal Medicine [39]. This test was found to be successful in spite of differences in the physician's attire, picture background, facial expression and age, as indicated in Figure 9. The IBM Watson visual recognition analytics tool [8] was able to overcome the above-mentioned hurdles and achieve descent match scores. The biometric validation for a HealthGrades physician image profile against the corresponding ABIM.org [30] profile returned a matching score of 0.59 via IBM Watson analytics, as shown in Figure 10.

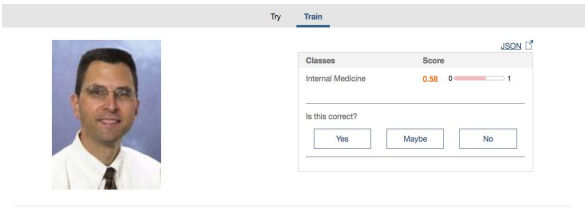

Fig. 6. Image Profile Matching Score for Erik Anderson, MD.

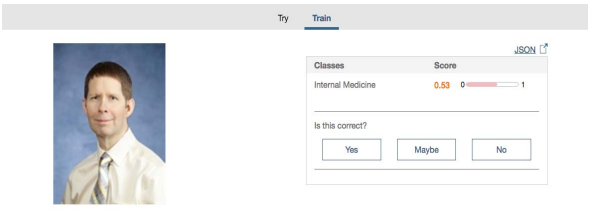

Fig. 7. Image Profile Matching Score for Regis Chamberlain, MD.

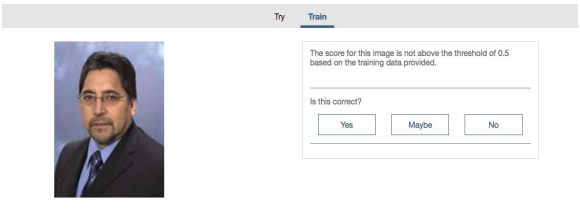

Fig. 8. Image Profile Matching Score for Alberto H. Araya, MD.

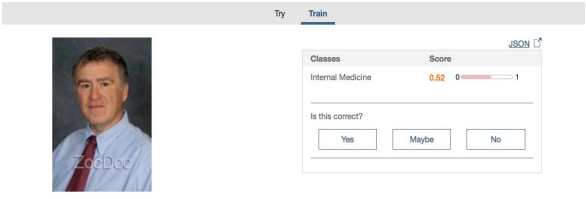

Fig. 9. Image Profile Matching Score for William J. Montesano, MD.

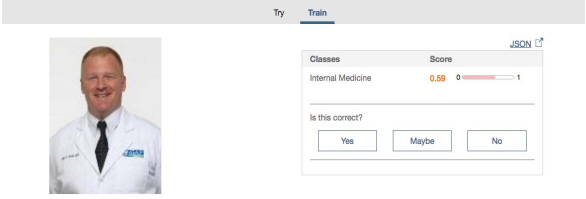

Fig. 10. Image Profile Matching Score for Brian S. Smith, MD.

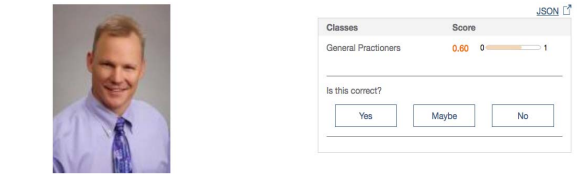

Fig. 11. Image Profile Matching Score for Douglas P. Galuk, MD.

There were multiple images from the Aspirus database [38] that were not recognized by IBM Watson visual recognition analytics [8], thereby yielding a biometric profile matching score below the threshold of 0.5 (one instance of such being displayed in Figure 8 screenshot). Some possible explanations of this experimental failure can be attributed towards image resolution discrepancies or a difference in image quality. It should be noted that all of the profile images provided on the HealthGrades website [29] were of significantly less quality than those pulled directly from the Aspirus database [38]. This resulted in IBM Watson analytics returning visual recognition match scores of an average of 0.57. Differences in both image size along with resolution quality were the most influential variables in the scores returned. Images with a relatively higher resolution and size (like the one in Figure 11) scored up to four tenths higher than those of poorer quality.

Subsequent adjustments of image resolution and size modification for both the Aspirus images and the HealthGrades photo profiles proved to be ineffective as it was found to have no effect on the resulting match scores. For instance, modifications to the HealthGrades image of Douglas P. Galuk, MD (as exhibited in Figure 11) for image quality enhancement yielded no change in the performance of IBM Watson analytics. The same original matching score of 0.60 was returned, despite altering the image size to 2592 by 3888 pixels to match the exact resolution and size of the corresponding Aspirus image. A resizing of successfully recognized images down to 25 by 33 pixels demonstrated that it was the minimum threshold pixel size for successful recognition by IBM Watson analytics (while validating images of that size, IBM Watson did not return a match score of above 0.5).

Other image recognition failures were seen due to images of significantly differing content, including elements such as the physican's age, attire, image quality, background and the picture style. A direct comparison of such images has been provided next to illustrate and explain the validation failure. In Figure 12, a side by side comparison can be seen of the "validator" and "validated" images for Shelbe Healy, MD. Both of these images were of satisfactory quality in terms of pixel size and image quality. However, IBM Watson failed to provide a positive recognition (as shown in Table I), due to not only the different attires and appearances of the involved physician in each of the pictures, but also due to the age difference and background changes.

Fig. 12. Shelbe Healy, MD: Aspirus (Left) and HealthGrades (Right)

The absence of glasses may also be of note as another reason of IBM Watson's non-match in this case. However, on the contrary, even with the case of Dr. William J. Montesano (as indicated by Figure 9) having a different pose, attire, and a slightly different appearance, IBM Watson analytics had still made a successful recognition. With the current image matching algorithms available in the visual recognition demo platform of IBM Watson, and the restriction on classifier file size, it is possible that IBM Watson is presently not capable of distinguishing major visual appearance differences such as the absence of glasses. Figure 13 points out an instance of difference between the "validated" and "validated" image quality (in terms of pixels). This image was pulled from the HealthGrades website and is inferior compared to the corresponding Aspirus profile, which is demonstrated in the left hand side picture's blurriness. IBM Watson analytics failed to make a match for both of these images due to the image quality differences, as evident here.

Fig. 13. David Tange, MD: HealthGrades (Left) and Aspirus (Right).

Despite failing to provide a positive recognition for images in which image attributes varied too greatly in terms of content and image quality, IBM Watson analytics was able to return a high score of 0.60 for the image authentication for Richard Wessling, MD, as depicted in Figure 14. While both of the "validator" and "validated" images possessed different qualities in terms of the age, clothing, pose and background, the image quality was quite high with a size of 1200 by 1500 pixels. Due to the image quality of the validating Aspirus image, IBM Watson was able to match the facial features of the physician while scanning through the images with differing backgrounds, and different depictions of age plus clothing.

Fig. 14. Richard Wessling, MD: Aspirus (Left) and HealthGrades (Right).

Other physician images, which obtained a high IBM Watson score of 0.59 or greater (such as the images of Douglas

Galuk, Rebecca Padilla, Patrick Allen and Thomas Smedberg), had validating Aspirus database images that had a high resolution (pixel count), with each measuring over 740 by 1000 pixels. Each of the corresponding validated reference website images from HealthGrades for each of the above physicians was either at or above the average 90 by 120 pixels.

From these image analyses, it is clear that higher image quality is needed to produce greater matching scores in visual recognition. Therefore, it is quite reasonable to state that for enabling success of the proposed biometric trust computational model, the published physician profile images need to comply with a set of image standards or guidelines. Ideally, for a successful authentication process, the visual profiles of providers need to be in accord amongst all online instances of their occurrences, which include "validator" and "validated" web sources. This means that the physicians (or providers) also need to play a part here by trusting and endorsing the OHI sites that post their profiles. Therefore, the proposed model will pave the potential path for development of trust at both the user and provider levels.

IV. Facial Recognition Based Biometrics As A Viable OHI Trustworthiness Indicator

After conducting the prototype verification experiment with the collected physician images from some sample OHI websites [28, 29] against a certified provider network of images using IBM Watson's visual recognition analytics tool based biometric authentication [8], the successful visual profile matching rates, as obtained and reported in Table I, indicate the prospects of the proposed biometrics based provider profile authentication model. Thus, the tabular results illustrate that visual recognition based biometrics can potentially act as a viable healthcare service provider-centric trustworthiness indicator for verifying OHI credibility and improving information assurance at the trustee or institutional level. An overall eighty-five percent (85%) success rate for biometric matching was attained with successful visual recognitions for 17 out of 20 images, as seen in Table II. The images obtained from HealthGrades [29] when tested and validated against the Aspirus database [38] resulted in a success stats of eighty-three point three percent (83.3%), as shown in Table III.

TABLE I. IBM Watson's Visual Recognition Analytics Based Biometric Research Findings: Image Wise Physician Profiles, Sources and The Corresponding Matching Scores

Physician	**IBM Watson Visual Recognition Data Analytics**		
	Selected OHI Reference Website (Validated Image Source)	***Provider Class Image Profile Source for Validation***	***Match Score***
Erik Anderson	HealthGrades.com [29]	Aspirus [38]	0.58
Regis Chamberlain	HealthGrades.com [29]	Aspirus [38]	0.53
Alberto Araya	HealthGrades.com [29]	Aspirus [38]	< 0.5
William J. Montesano	ZocDoc.com [28]	Greater Rochester Internal Medicine [39]	0.52
Brian S. Smith	HealthGrades.com [29]	ABIM [30]	0.59
Tyler Beckley	HealthGrades.com [29]	Aspirus [38]	0.59
Kevin Ferreira	HealthGrades.com [29]	Aspirus [38]	0.55
Douglas Galuk	HealthGrades.com [29]	Aspirus [38]	0.60
David Tange	HealthGrades.com [29]	Aspirus [38]	< 0.5
Rebecca Padilla	HealthGrades.com [29]	Aspirus [38]	0.59
Shelbe Healy	HealthGrades.com [29]	Aspirus [38]	< 0.5
Patrick Allen	HealthGrades.com [29]	Aspirus [38]	0.59
Laurence Gordon	HealthGrades.com [29]	Aspirus [38]	0.55
Matthew Clark	HealthGrades.com [29]	Aspirus [38]	0.56
Daniel Priebe	HealthGrades.com [29]	Aspirus [38]	0.59
Elizabeth Barr	HealthGrades.com [29]	Aspirus [38]	0.58
Cody Nikolai	HealthGrades.com [29]	Aspirus [38]	0.59
Bradley Boettcher	HealthGrades.com [29]	Aspirus [38]	0.54
Thomas Smedberg	HealthGrades.com [29]	Aspirus [38]	0.59
Richard Wessling	HealthGrades.com [29]	Aspirus [38]	0.60

TABLE II. Summary of Ibm Watson's Visual Recognition Analytics Based Biometric Research Findings: Overall Image Source Wise Physician Profile Matching Instances

Provider Class Image Profile Source for Validation	***Selected OHI Reference Website (Validated Image Source)***	***Number of Matches***	***Number of Non-Matches***
Aspirus [38]	HealthGrades.com [29]	15	3
Greater Rochester Internal Medicine [39]	ZocDoc [28]	1	0
ABIM [30]	HealthGrades.com [29]	1	0

TABLE III. SUMMARY OF IBM WATSON'S VISUAL RECOGNITION ANALYTICS BASED BIOMETRIC RESEARCH FINDINGS: OVERALL IMAGE SOURCE WISE SUMMARIZED PHYSICIAN PROFILE MATCHING STATS

Provider Class Image Profile Source for Validation	***Selected OHI Reference Website (Validated Image Source)***	***Overall Image Profile Matching Statistics***
Aspirus [38]	HealthGrades.com [29]	83.3%
Greater Rochester Internal Medicine [39]	ZocDoc [28]	100%
ABIM [30]	HealthGrades.com [29]	100%

IBM Watson visual recognition analytics demonstrated the ability of correctly matching physician profile pictures from different third party sources [28, 29] when validated against a corresponding provider network of images [30, 38, 39]. It also recognized and authenticated in tricky cases of verification, for instance when two photographs in comparison were not quite exactly alike, as seen in the given example of Figure 14, and in the corresponding experimental result shown in Table I. These observations suggest that the OHI trust formation can be enhanced at the user or trustor level (information assurance through verification) and the provider or trustee level (affiliation and endorsement by provider) by applying biometrics and implementing visual recognition driven authentication. Hence, the proposed biometric authentication based trust computational model will provide information assurance through validation of the physician profiles affiliated with the third party OHI that consumers are reading or seeking.

Overall, the above IBM Watson visual recognition analytics based experiments enabled us to arrive at the following noteworthy points:

- Profile picture uniformity and consistency (in terms of image quality) across multiple OHI websites is required in order to obtain the most accurate visual recognition based biometric validation results
- Images of a greater quality yield a higher visual recognition score than those of inferior quality, and this leads to a demand of better quality profile images
- Classifier images of better quality from provider network sources enables stronger performance in biometric authentication and allows for greater variation and compromise in the quality of the reference OHI website profile images under validation
- Adjusting and upgrading of image resolution plus size of inferior/poor quality images from reference OHI websites yields no improvement in IBM Watson's visual recognition based analytical performance

V. CONCLUSION: OVERALL SUMMARY AND THE FUTURE

The main contribution of this paper is a novel biometric authentication based hybrid trust-computing model that innovates OHI trust related research by exploiting a unique provider-centric approach and verifies trust constructs at the institutional level. This first of its kind provider-profile based biometric authentication model can be used to expand the trust of online healthcare consumers on OHI content (involving third party websites). In a way, this innovative model can also help to extend the trust of healthcare providers on the OHI websites (involving third parties) by indirectly advocating for collaboration between healthcare providers and the third part OHI website owners. The presented work represents a unique application of computer vision based visual recognition biometrics to the field of information assurance based trust computation in OHI.

The real-life implementation process of the proposed model would become much easier and get a boost to serve its intended purpose, if the providers would actually endorse the OHI content of the third party websites, and share their authentic institutional profiles. However, since this proposed model uses physician image profiles to effect visual recognition driven biometric validation, its successful implementation depends on the existence of online visual profiles for physicians as well as on the quality plus resolution of the images. The conducted research experiments with IBM Watson's visual recognition based analytics [8] reveal that the provider image profiles, as used with OHI, need to conform to certain minimal standards of resolution and quality. These observations along with the experimental dataset of the provider images would act as valuable inputs and research knowledge base for future work in this area.

The research conducted in this paper seeks to explore the trustworthiness of OHI through verification of provider profiles via visual recognition based cross-validation. In the process, it investigates OHI elements and attributes that are connected to the perception of trust building through biometric authentication. One of the limitations that came up in the scope of our research was the inconsistency in the use of actual provider image profiles in the OHI domain websites. Another challenge faced during the experiments was the lack of quality provider images, given that a lot of the collected provider images from OHI websites were of low resolution and poor image quality. Thus, this research indirectly lobbies for publishing more visual provider profiles of better quality in the OHI domain. Thus, this project work sets up the foundation for further research on hybrid-trust driven policy-making in online healthcare consumerism [40].

Next plan of action in this research project is the creation of a prototype software application that shall represent a functional tool for automation of the biometric authentication process presented in this paper. Future research and development work shall also involve design and development of an actual OHI trust metric that generates more meaningful and holistic trust scores for online health consumers. Other potential future work includes deployment of the presented OHI trust-computing model with the actual healthcare community, including online healthcare consumers and providers in an effort to collect feedback data from the OHI users and providers as part of the research study as to whether the proposed model can improve trust and counter cyberchondria. Lastly, the use of pattern recognition techniques for verifying OHI website logo affiliations could be a possible step for another potential hybrid trust-computing approach in this sector. Overall, given the prolific use of OHI

websites by today's consumers, it is imperative that a resource for determining the credibility, authenticity and trustworthiness of OHI be developed. The prototype model presented here would represent the first technical hybrid model exploiting both "soft trust" and "hard trust" markers to validate and verify OHI websites in order to determine their credibility.

REFERENCES

[1] S. Fox, "Mobile Health 2010," Pew Internet and American Life Project.

[2] A. M.. Barbara, M. Dobbins, R. B. Haynes, A. Iorio, J. N. Lavis, P. Raina, and A. J. Levinson, "The McMaster Optimal Aging Portal: Usability Evaluation of a Unique Evidence-Based Health Information Website," *JMIR Human Factors* 3, no. 1, (2016).

[3] E. Brainin, and E. Neter, "Inside Technology: Opening the Black Box of Health-Website Configuration and Content Management," *Future Internet 6*, no. 4, (2014): 773-799.

[4] K. L. Turkiewicz, "Cyberchondria scale construction: The Cyberchondria Assessment Measure (CYCAM), " Paper presented at the Central States Communication Association Conference, Cleveland, OH. Health Communication Interest Group, (2012).

[5] R. W. White, and E. Horvitz, "Cyberchondria: Studies of the escalation of medical concerns in web search," ACM Transactions on Information Systems, 27, 1-37, (2009).

[6] K. Muse, F. Mcmanus, C. Leung, B. Meghreblian, and J. M. G. Williams. "Cyberchondriasis: Fact or fiction? A preliminary examination of the relationship between health anxiety and searching for health information on the Internet," *Journal of Anxiety Disorders* 26, no. 1 (2012): 189-96, (2009).

[7] V. Starcevic, and E. Aboujaoude, "Cyberchondria, Cyberbullying, Cybersuicide, Cybersex: "New" Psychopathologies for the 21st Century?" *World Psychiatry*, 14(1):97-100. doi: 10.1002/wps.20195, (2015).

[8] "IBM Watson Visual Recognition Demo," *IBM*. N.p., 2017. Web. 5 Jan. 2017. Print. https://visual-recognition-demo.mybluemix.net/.

https://www.ibm.com/watson/developercloud/doc/visual-recognition/index.html.

[9] A. H. Alpaslan, "Cyberchondria and adolescent," *Social Psychiatry* 1, (2016): 2.

[10] E. Sillence, P. Briggs, and P. R. Harris, "Healthy persuasion: web sites that you can trust," *Persuasive Technology and Digital Behaviour Intervention Symposium*, (2009).

[11] M. Khosrowjerdi, "A review of theory-driven models of trust in the online health context," *IFLA journal 42*, no. 3, (2016): 189-206.

[12] H. Singal, and S. Kohli, "Trust Necessitated through Metrics: Estimating the Trustworthiness of Websites," *Procedia Computer Science 85,* (2016): 133-140.

[13] J. Sänger, and G. Pernul, "TRIVIA: visualizing reputation profiles to detect malicious sellers in electronic marketplaces," *Journal of Trust Management 3*, no. 1, (2016): 5.

[14] P. Kostagiolas, N. Korfiatis, P. Kourouthanasis, and G. Alexias, "Work-related factors influencing doctors search behaviors and trust toward medical information resources," *International Journal of Information Management 34*, no. 2, (2014): 80-88.

[15] M. N. Yap, M. Kamalrudin, A. Z. A. Bakar, and S. Sidek, "Verification on the Trustworthiness of Information: A Study," *Journal of Theoretical and Applied Information Technology 92*, no. 1, (2016): 72.

[16] G. Giasemidis, C. Singleton, I. Agrafiotis, J. RC Nurse, A. Pilgrim, Chris Willis, and D. V. Greetham, "Determining the veracity of rumours on Twitter," *International Conference on Social Informatics*, pp. 185-205. *Springer International Publishing*, 2016.

[17] F. Pauer, J. Göbel, H. Storf, S. Litzkendorf, A. Babac, M. Frank, V. Lührs et al., "Adopting Quality Criteria for Websites Providing Medical Information About Rare Diseases," *Interactive Journal of Medical Research 5*, no. 3, (2016).

[18] Y. Kim, "Trust in health information websites: A systematic literature review on the antecedents of trust," *Health informatics journal,* (2014): 1460458214559432.

[19] A. J. Lazard, and M. S. Mackert, "E-health first impressions and visual evaluations: key design principles for attention and appeal," *Communication Design Quarterly Review 3*, no. 4 (2015): 25-34.

[20] F. Johnson, J. Rowley, and L. Sbaffi, "Modelling trust formation in health information contexts," *Journal of Information Science,* (2015): 0165551515577914.

[21] E Sillence, and P. Briggs, "Trust and Engagement in Online Health A Timeline Approach," *Handb PsycholCommun Technol 33,* (2015): 469-87.

[22] A. Bakke, "Ethos in E-Health: From Informational to Interactive Websites," *Establishing and Evaluating Digital Ethos and Online Credibility* (2016): 85.

[23] L. C. Vega, T. DeHart, and E. Montague, "Trust between patients and health websites: a review of the literature and derived outcomes from empirical studies," *Health and technology* 1, no. 2-4 (2011): 71-80.

[24] E. Sillence, and P. Briggs, "The Evolution of Trust in a Design Contex," *Design and semantics of form and movement 30,* (2007).

[25] V. Rafe, and M. Monfaredzadeh, "A qualitative framework to assess hospital/medical websites," *Journal of Medical Systems 36*, no. 5, (2012): 2927-2939.

[26] C. L. Corritore, S. Wiedenbeck, B. Kracher, and R. P. Marble, "Online trust and health information websites," *International Journal of Technology and Human Interaction (IJTHI) 8*, no. 4, (2012): 92-115.

[27] A. Chattopadhyay, "Developing an Innovative Framework for Design and Analysis of Privacy Enhancing Video Surveillance." PhD diss., *University of Colorado Colorado Springs. Kraemer Family Library*, 2016.

[28] "Zocdoc," *Zocdoc*. N.p., 2017. Web. 10 Jan. 2017. https://www.zocdoc.com/.

[29] "Healthgrades Find A Doctor | Doctor Reviews | Hospital Ratings," *Healthgrades*. N.p., 2017. Web. 9 Jan. 2017. https://www.healthgrades.com/

[30] "Home | ABIM.Org," *Abim.org*. N.p., 2017. Web. 9 Jan. 2017. http://www.abim.org/.

[31] M. Kuo, "Opportunities and challenges of cloud computing to improve health care services," *Journal of medical Internet research 13*, no. 3 (2011): e67.

[32] G. Athanasiou, and D. Lymberopoulos, "A comprehensive Reputation mechanism for ubiquitous healthcare environment exploiting cloud model," *Engineering in Medicine and Biology Society (EMBC)*, 2016 *IEEE 38th Annual International Conference*, pp. 5981-5984, 2016.

[33] I. Martínez-Sarriegui, F. García-García, G. García-Sáez, M. E. Hernando, and M. Luck, "TRHIOS: Trust and reputation in hierarchical and quality-oriented societies," *Information Systems and Technologies (CISTI)*, 2012 *7th Iberian Conference*, pp. 1-4. IEEE, 2012.

[34] S. S. Msanjila, and H. Afsarmanesh, "On hard and soft models to analyze trust life cycle for mediating collaboration," *Working Conference on Virtual Enterprises*, pp. 381-392. Springer Berlin Heidelberg, 2009.

[35] C. Lin, and V. Varadharajan, "A hybrid trust model for enhancing security in distributed systems," *Availability, Reliability and Security,* (2007). ARES 2007. *The Second International Conference on*, pp. 35-42. IEEE, 2007.

[36] A, Beldad, M. De Jong, and M. Steehouder, "How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust," *Computers in Human Behavior 26*, no. 5 (2010): 857-869.

[37] H. Singal, and S. Kohli, "Mitigating Information Trust: Taking the Edge off Health Websites," *International Journal of Technoethics (IJT) 7*, no. 1 (2016): 16-33.

[38] "Home | Aspirus Main,"*Aspirus.org*. N.p., 2017. Web. 18 Mar. 2017. http://www.aspirus.org.

[39] "Greater Rochester Internal Medicine," *Grinternalmedicine.com*. N.p., 2017. Web. 18 Mar. 2017. http://www.grinternalmedicine.com.

[40] A. Chattopadhyay, and K. Turkiewicz, "Future Directions In Online Healthcare Consumerism Policy Making: Exploring Trust Attributes Of Online Healthcare Information | IEEE Internet Initiative," *Internetinitiative.ieee.org*. N.p., 2017. Web. 24 Mar. 2017.