Several Emerging Information Technology Topics and Related Doctoral Dissertation Ideas

S. Cicoria, J. Sherlock, M. Muniswamaiah, L. Clarke, G. Crocetti, M. Coakley, P. Dressner, W. Kellum, T. Lamin, S.Feddock, J. Flynn, M. Kirchhoff, N. Nassar, J. Sicuranza, T. Johnson, J. Navarro, I. Idiong, and M. Weeks
Seidenberg School of CSIS, Pace University, White Plains, New York

***Abstract*—Information technology is emerging on many fronts. Spectators, scientists and researchers are anticipating a faster pace of technological advancement turning our day to day interaction into a mesh of connected devices. Internet of Things (IoT) is where we are driving toward, and these connected 'things' encapsulate four main areas. Identity and how this is turning into a service to accommodate the upcoming wave of connected devices, wearable devices, Crypto-Currency which is the futuristic currency flowing between these emerging technologies and the new emerging concept of big data.**

I. Introduction

A look at Identity as a Service (IDaaS) and Federated Identity Management (FIM) and acceptance amongst organizations, users, and general population. While FIM has shown acceptance amongst educational, commercial and government organizations, the general population acting has not seen the level of trust as the former. What are the barriers or enablers for acceptance that might allow, in the extreme example, the ability to logon to a bank with your Facebook credentials and transact business?

Wearable devices, or 'wearable' for short, have enormous potential for uses in health and fitness, navigation, social networking, commerce, and media. As we are marching forward with steady steps toward the Internet of Things, IOT, wearable technology is playing a major role introducing smart gadgets that is light and interactive with our day to day lifestyle.

Simply put a crypto-currency is money that has been converted to a value expressed in bits and encoded for secrecy. In ways it is similar to using an ATM. This presentation will illuminate differences by making it clear how crypto-currency works. One common protocol for crypto-currency is Bitcoin. There are no coins per se except in the expression but there are bits. The said money can then be exchanged using the internet for payment of debts or other commercial purchases pseudonymously.

A look at how big data is transforming telemedicine to provide better care by tapping into a larger source of patient information. Telemedicine will have a profound impact on patient care, increase access and quality, and represent an opportunity to keep health care costs down. Data generated by smart devices will enable the real-time monitoring of chronic diseases, allowing optimal dosage of drugs and improve patient outcomes.

II. ID as a Service, IDaaS

Many solutions, products, and protocols exist for establishing federated identity for enabling users to securely logon to Service Providers (SP) for various purposes, yet, there is still a chasm with regards to trust. That is whether consumers trust both Identity Providers (IdP) and SP to participate in a federation.

We take a look at research that examines commercial and public organizations and various implementation impediments and facilitators. Additionally, while Federation amongst universities, government, and, commercial partners is much more prevalent, we lack that level of acceptance for the general population. We take a look at government efforts, most notably in the European Community towards establishing a common credential provider and broker-based approach.

Finally, for future research, we ask a rhetorical question – when will I be able to use my Facebook Identity to logon to my bank?

A. Federation identity basics

Initially organizations started to use Single-Sign-On (SSO) to unify authentication systems together for better management and security. SSO was adopted across different internal applications and via APIs for external applications. With platforms spread across different devices bringing in together user authentication and authorization

with increased security is a challenge which Federated identity tries to address [5].

In Federated identity an application uses an identity management system that stores user's electronic identity to authenticate. It decouples authentication and authorization functions. It avoids a situation where every application has to maintain a set of credentials for every user [5].

B. Government Sponsored Federation

Since 1995, EU member nations have been implementing various forms of electronic Identity Management (eIDM) based on the interoperability of eSignatures. The lack of an EU-wide legal framework governing such an implementation has resulted in difficulties in defining actor responsibilities and liabilities. Cross-border requirements amongst EU countries have created incremental challenges. This has unfortunately resulted in a degree of "subsidiarity" amongst the member nations: each member nation maintaining its autonomy and responsibility. [1]

Both the U.S. and the U.K. governments have decided that citizens will authenticate to government resources using Federated Identity; however, neither government wishes to perform the role of IdP[1]. This defers to private industry the opportunity to offer identity management solutions to consumers while still not answering questions such as (1) who will oversee the solution design and implementation, and (2) who will control and monitor the governance of the solution. What limited functionality has been implemented on the consumer side in the UK has been received with a reasonable level of trust on the part of the consumer, with ease-of-use scoring the highest. Opportunities have been identified[1]:

- 50% left the site once reaching the hub page,
- 25% left the site once reaching the consent page,
- 34% of users felt threatened, not reassured, by the privacy.

C. InCommon – Where it's working

Within the U.S. driven by the research community, "The InCommon Federation is the identity management federation for US research and education, and their sponsored partners" [2]. They currently service over 7.5 Million users with this federation amongst 430 education and nearly 200 other organizations[2].

The success of InCommon may be linked back to the Shibboleth model that was implemented, along with Trust in Privacy from the IdPs and alleviation of significant identity management functionality for SP[3]. This also was a step-up for many organizations in having better security than previous implementations. For example, JSTOR had been using IP address blocks to permit access from users cross Universities. The implementation of InCommon using Shibboleth allowed clarity in who is requiring access with some level of assurance that the actual user has been authenticated and permissioned for access by the supplying IdP amongst the trust.

D. Consumer Federation

What may be core to the success of InCommon is a captive community of practitioners that utilize the services offered within the Federation for their daily needs. It may also be attributed to a community well versed in the underlying technology, or at least comfortable with it in general. We still haven't seen the ability to access your Bank Account through this federation.

Amongst the general population we have different motivations that may attribute to the slow uptake or resistance. In the UK, the Identity Assurance (IDA) program issued guidelines and mandates for implementation of an approach that has yet to take hold[1].

In a series of studies[1] various obstacles were cited ranging from poor User Interface Design, to Security and Trust concerns. Major concerns still exist over unauthorized release of privacy information, along with inability to understand associations of an IdP to a SP – one stating "PayPal have nothing to do with the National Health Service (NHS)"[1].

The lack of general Trust in the federation amongst the general public may be attributed to their naivety or lack of understanding of the overall Federation model. The same study suggests that this may be improved through better User Experience (UX) and also presents as part of that argument which examples of UX worked better or worse in their studies[1].

The same study also identifies which types of IdPs seem more trustworthy, or may be a candidate for use within a Federation scenario amongst the general population, with the post-office and cable providers being amongst the highest potential for "Would use" in a Federation scenario[1].

Establishing eIDM trust in the eyes of the general population has presented itself as a significant barrier to full scale end-to-end implementation of Federated Identity. These roadblocks include issues such as:

- No clear definition on what constitutes an eID,
- Disagreement on which governing body (governmental or private) should create and manage the eID,

- Disagreement on which governing body should manage and/or regulate the data flows amongst the various FIM SP,
- How the integrity/reliability/privacy of the identity will be ensured; who will stand behind this guarantee.

F. Risks

Trust, security and liability are three key areas of risk which are constantly challenged with FIM/IDaaS systems. The trustworthiness of the user, the IdP or SP may be in question by the entity who did not perform the identity screening. The development of the NIST[7] identity credentialing via the service levels is one method to assist SP and IdP in properly screening their members.

From a security perspective, Man-in-the-Middle attacks in an open network can lead to theft on identity credentials which allow access to confidential information. Misuse of the IdP and SP with user identity information causing the risk of IdP becoming malicious and risking the use of user identity information in SPs to share it with other SPs or third parties.[6]

In many of the types networks where FIM/IDaaS systems have been tried the questions always arises, what happens if something goes wrong? Or more importantly, who is liable? A system could become unavailable to authenticate users, causing problems for SP relying on its operation. And authentication itself could fail, allowing unauthorized users to be incorrectly authenticated as other users. In both cases, rules that determine which party is responsible are a potential source of conflict.[3] Liability arrangements must be clearly defined and articulated for all stakeholders.[3]

G. Summary and further research

Globally, there is consensus that new research would be needed to coordinate existing knowledge and know-how into a coherent vision capable of being seamlessly implemented cross-border and cross-culture, spawning the required trust and confidence at all levels. [4]

A number of conceptual models exist which demonstrate that there is a need for a unified solution to federated identity management: for individuals, businesses and government agencies alike. These technological solutions have been proven to be viable and cost effective for many of today's e-commerce environments, yet full scale implementation is constrained by a low level of trust on the part of the general population of the technology and of the SPs. Partly the result of misinformation and misunderstanding, many of the FIM participants would be more inclined to participate in these eIDM offerings if they could only get beyond the trust issues.

Further research would be required to address consumer concerns:
- Who should 'own' (i.e. regulate) the solution?
- What would it take to raise confidence in any solution?
- What is the model for user recourse if the solution breaks?

Reviews of current state of eID implementations indicate that, at least for the short term, consumers may not be able to use a common access/authentication method for secure online resource access control.

III. WEARABLE TECHNOLOGY

Wearable devices, or 'wearable' for short, have enormous potential for uses in health and fitness, navigation, social networking, commerce, and media. As we are marching forward with steady steps toward the Internet of Things, IOT, wearable technology is playing a major role introducing smart gadgets that is light and interactive with our day to day lifestyle. In this section, we will introduce latest wearable technology in three main sections: Health and Fitness, Security, and lifestyle accessories.

A. Medical devices

Wearable surveillance system; Wearable Belt that monitor variations of posture, falls, and gait disability. These devices contain communication Module: Wireless LAN card; Connects to Users Home Network and a storage Module that is about 256MB as a memory card. On top of that, they include an analysis module to provide the decision making capability and of course a sensor module that is used for data gathering. Also medical sensors that provide early alert to medical staff contains firmware is fitted in the insole and communicates with PC software via USB radio stick

We can always see the positive side of these devices such as monitoring daily activities and change in activities for notifications in addition, freedom of movement, daily wear, comfortable, improve performance, monitor rehabilitation. Some considered that it is discomfort while sleeping

B. Fitness devices

Wearable fitness devices seem to be everywhere. From Nike's FuelBand to Jawbone's Up to the Fitbit Flex and now Samsung's new Gear Fit, it feels like everyone is slapping one on their wrists with the hopes of changing their workout habits for the better. These devices are using Wireless Bluetooth 4.0 to synch to computer, iPhone, and/or Android Smartphones. While many believes that they are great to see real time progress and daily stats on wrist and watch progress over time with charts and graphs. Also, set daily goals, earn badges, challenge friends. Some consider the Wristband hard to clasp and some rashes have been reported. In addition, in some cases, metrics not accurate. [22]

C. Wearable Security

As wearable devices potentially being used in many aspects of life, security is no difference. Many companies jumped on that wagon and wearable devices are used for authentication and for authorization. In some cases, wearable is potentially a password replacement, a tracking device for Child/Pet Protection.
Commonly wearable security devices use NFC & Bluetooth to 'lock' mobile device once user leaves proximity. Also it contains algorithms to identify its associated ACL of programs. Recently, researchers are considering taking one heart's unique rhythm and creating a secure ID for you from it[24]

Among many of the benefits of wearable security devices, knowing where pet's or children's whereabouts, Seamless Authentication to Devices, cars, Hotel Rooms, etc, and true biometric, cannot be copied, and useless if lost

D. Wearable Accessories

Many considered wearable devices are mainly for convenience. As a results, enterprise didn't wait too long to come up with wearable devices that target technical savvy and luxury life style. Smart watches like Sony SmartWatch, Apple iWatch, Galaxy Gear are a living proof since they are low hanging fruit to manufacture. They are mainly using smart phone technology, and depends on NFC, Bluetooth, and RF technology for communication. This provide more integration, gateway to Internet of Things (IOT). However, many consider them distraction on the road, and they also still have fairly limited battery life, let alone the smaller screens that doesn't seem able to display much if information[22].

While Google pioneered in many new technologies, they couldn't let wearable technology wave passes without jumping on it. Google glass is termed as a wearable computer, developed by Google X Lab. The glasses are used to display information in a smart phone-like hands –free format that can interact with the internet via natural voice command. Also it contains eye tap technologies. Android technology with 4G [20][21].

Google Glass provide an experience known as augmented reality, where images are superimposed over what the user see in real life. One thing is limiting the glassed from spreading among many demographic groups is the geeky look. These devices aren't airport-friendly. Many consider those who wear them publicly have a 'Nerdy' look and often falls under a social stigma.

E. Research Areas

Acute illness with medical wearable devices where patients are treated by devices that operating in their bodies to detect illness or pacify pain. Also pharmaceutical industry will be revolutionized with the wearable pill which tells doctors when it's been swallowed and any impact on the body. With these devices operating inside the human body, the need for power (even low level power source) is a must have. Therefore, Edible micro-battery that could power ingestible medical devices is also an area of study and research. These devices could be a hazardous if they were not well managed. Since the point for these devices is to communicate with the body and with other devices, security plays a major role to ensure that no unauthorized access is granted. That also includes Wearable devices' authentication and How to handle unsecure networks and hostile environments.

IV. CRYPTO CURRENCY

In 2009 specifications and a proof of concept7 for Bitcoin was published by Satoshi Nakamoto. This was the first truly cryptocurrency. This point is where the popular press picks up the history of Bitcoin. The truth is there was a long trail of contributors before Nakamoto and Bitcoin: DigiCash begun in 1990 by David Chaum purchased by Ecash in 1998 absorbed by InfoSpace in 2002 [14]. Speculation arose starting with a paper written in 1985 of a transaction system without identification that was secure2 by David Chaum followed in 1988 with a second

paper about untraceable electronic cash3. He wrote his first paper on this subject in 1982 [14]. By the early 90's two papers appeared that tied together two concept that became key for crypto-currency: Universal Electronic Cash [11] and Wallet Databases with Observers [12]. In 1996 the cryptographic means of security was described in The Cryptography of Anonymous Electronic Cash[6] by the enigma known as Satoshi Nakamoto

A. How does it work?

Public-Key Cryptographic Tools

One-Way Functions: The function phi is one-way if, given s in the domain of phi, it is easy to compute t=phi(s), but given only t, it is hard to find.

Key Pairs: If phi is one-way function, then a key pair is a pair s, t related in some way via phi. We call s the secret key and t the public key. Each user keeps his secret key to himself and makes his public key available to all. The secret key remains secret even when the public key is known, because the one-way property of phi.

Digital Signature: A user identifies himself by proving that he knows his secret key without revealing it. This is done by performing some operations using the secret key which anyone can check or undo using the public key (identification). If one uses a message as well as one's secret key, one is performing a digital signature on the message.

Secure Hashing: A hash function is a map from all possible strings of bits of any length to a bit string of fixed length. If a hash is both one-way (to prevent signature forgery) and collision-free (to prevent repudiation), it is said to be a secure hash.

Untraceable Electronic Payment such as

Blind Signature: It is necessary that the Bank not be able to link a specific withdrawal with a specific deposit. This is accomplished by using a special kind of digital signature called a blind signature.

Blinding: In the withdrawal step, the user changes the message to be signed using a random quantity. This step is called blinding the coin, the random quantity is called the blinding factor.

Unblinding: The Bank signs this random-looking text, and the user removes the blinding factor (unblinding). The user now has a legitimate electronic coin signed by the Bank. The Bank will see this coin when it is submitted for deposit, but will not know who withdrew it since the random blinding factors are unknown to the Bank. Bank does not know what is signing in the withdrawal step. The Bank uses secret keys for fixed amounts (one key for a $10 withdrawal, another for a $50 withdrawal, and so on).

Basic Electronic Cash Protocol

Payment Anonymity: Neither payer nor payee should know the identity of the other. This makes remote transactions using electronic cash totally anonymous.

Multiple Spender: If a merchant tries to deposit a previously spent coin, he will be turned down by the Bank, but neither will know who the multiple spender was since she was anonymous.

Identifying Information: The payer shares some sort of identifying information with the payee at the payment step, in addition to her electronic coin. This information is created during the withdrawal step. The withdrawal protocol includes a step in which the Bank verifies that the information is there and corresponds to Alice and to the particular coin being created.

To preserve payer anonymity, the Bank will not actually see the information, only verify that it is there. Alice carries the information along with the coin until she spends it.

Challenge-Response Protocol: Bob sends Alice a random challenge quantity and, in response, Alice returns a piece of identifying information. At the deposit step, the revealed piece is sent to the Bank along with the coin. If she spends the coin twice, the Bank will eventually obtain two copies of the same coin, each with a piece of identifying information. If the piece of identifying information is the same, we know that her coin was copied and re-spent by someone else. If the piece of identifying information is different (due to the randomness in the challenge-response protocol), The Bank will be able to identify her as the multiple spender.

Withdrawal:	- Alice creates an electronic coin, including identifying information.

	- Alice blinds the coin. - Alice sends the blinded coin to the Bank with a withdrawal request. - Bank verifies that the identifying information is present. - Bank digitally signs the blinded coin. - Bank sends the signed blinded coin to Alice and debits her account. - Alice unblinds the signed coin.
Payment:	- Alice gives Bob the coin. - Bob verifies the Bank's digital signature. - Bob sends Alice a challenge. - Alice sends Bob a response (revealing one piece of identifying info). - Bob verifies the response. - Bob gives Alice the merchandise.
Deposit:	- Bob sends coin, challenge, and response to the Bank. - Bank verifies the Bank's digital signature. - Bank verifies that coin has not already been spent. - Bank enters coin, challenge, and response in spent-coin database. - Bank credits Bob's account.

Table 1. Off-line cash Protocol.

B. Challenges

The risk that a digital currency can be spent twice. Bitcoin has a mechanism based on transaction logs (publicly viewable) known as a "block chain" to verify the authenticity of each transaction and prevent double-counting.
When digital currency is exchanged, there is a very real possibility that the currency could be copied over to the recipient, with the 'original' still intact in the owner's possession. In this case, a currency-holder would be much more likely to take the risk of spending a unit of currency twice.

Sending a fraudulent transaction log to a seller and another to the rest of the Bitcoin network. Bitcoin transactions take some time to verify because the process involves intensive number-crunching and complex algorithms that take up a great deal of computing power. It is, therefore, exceedingly difficult to duplicate or falsify the block chain because of the immense amount of computing power that would be required to do so.

Transaction List, If P1 and P2 are XOR-ed the original id of the user will be revealed. But only the last owner can be seen, "CHARLIE." Note that secret sharing is done with XOR, not concatenation. Concatenation is used for illustration just to make the picture readable. There is no way the identities of ALICE and BOB can be extracted from the transaction list.

When a user spends their money, the protocol will randomly blank some of P1 and some of the P2 for the current owner, and adds another list of P1 and P2 for the new owner.

P1	P2
ALI	---
---	ICE
---	E
BO	---
---	OB
B	---
CHA	RLIE
CH	ARLIE
CHARL	IE

V. BIG DATA

Telemedicine refers to the use of modern telecommunication capabilities for medical information exchange between a care provider and patients in order to improve health outcome. Started out over forty years ago with the use of telecommunication technologies to extend hospital care to patients located in remote areas, telemedicine has spread rapidly and is now becoming integrated into the daily operations of hospital, specialty departments, home health agencies, and private physicians [15].

Telehealth solutions, promise to have a profound impact on patient care, its quality and safety, and can also help drive costs out of the healthcare system. For instance, enabling the chronically ill and elderly to receive care from home reduces the number of hospital admissions and readmissions, which are riddled with expense and risk of exposure to other illnesses.

A. Telemedicne as a service

Telemedicine is primarily an enabling technology which provides primary care and patient monitoring.

Primary care and specialist referral services may involve a primary care or allied health professional providing a consultation with a patient or a specialist assisting the primary care physician in rendering a diagnosis. This may involve the use of live interactive video or the use of store and forward transmission of diagnostic

images, vital signs and/or video clips along with patient data for later review.

Remote patient monitoring, including home telehealth, user devices to remotely collect and send data to a home health agency or a remote diagnostic testing facility (RDTF) for interpretation. Such applications might include a specific vital sign, such as blood glucose or heart ECG or a variety of indicators for homebound patients. Such services can be used to supplement the use of visiting nurses.

Consumer medical and health information includes the use of the Internet and wireless devices for consumers to obtain specialized health information and on-line discussion groups to provide peer-to-peer support [15].

The ubiquitous presence of mobile infrastructure even in developing country translates into improved access to health for people with limited interaction to health providers, filling an important gap in bringing health care into underserved and underprivileged communities. The easy access to telecommunication infrastructure also allows the possibility of training local health professionals through special medical education seminars remotely.

B. Big Data in Telemedicine

From wearable devices to nanotechnologies to self-tests, our life will soon be filled with a plethora of devices that will constantly monitor our health. These devices will constantly generate data that will be collected and analyzed real time.

Instead of sampling the data for analysis, systems will detect disease patterns on-the-fly and alert the patient and the doctor at the first sign of anomaly, which is particularly important for chronic illness like atrial fibrillation or blood clotting to name just a few [16].

The variability of this data will be so great that we will be able to detect differences on how the same disease affects different sub-population and administer the proper medication according to the proper phenotype. Through the use of wireless and nanotechnologies we will be able to administer the right drug, at the right level, at the right time by virtually eliminate side effects. This will be possible thanks to personalize medicine which is collecting a huge amount of genomic data to understand how drugs are metabolized differently by different people. [17]

The research team at the Mt. Sinai Hospital in New York, for example, is linking together the sequencing information of patients suffering of various forms of cancer and already identified genomic pathways for the development of novel therapeutic and diagnostic approaches for human diseases through integration and analysis of molecular and clinical data, and also perform research to develop and evaluate methods to incorporate genomic sequencing data into clinical practice [20].

More data allows the research and development of new and improved methods for the diagnosis, prevention, and treatment or rare and common genetic diseases.

C. Why Big Data Is Important

Big data usually includes data sets from diverse sources and with sizes well beyond the ability of commonly used software tools to ingest, manage, and process the data within an acceptable amount of time. The bad news, however, do not stop here: things will only get worst with data to grow 50 folds by 2020 [19].

Many industries are following this issue very closely, with some companies like Amazon, Google, and Netflix taking the lead in attacking the problem heads on.

For telemedicine this means the necessity, for the medical support staff, to extract the necessary data for patients to pass along to medical professional. The ability of processing such huge amount of information will translate into improved medical knowledge that benefits research and patient alike.

Big data represents a revolution in medical research and the time when we struggled to obtain samples in order to study a particular population are over. Today, with the availability of large and diverse datasets coming from many parts of the world allows us to consider the size of our sample as n=All: this will force a complete overhaul of our research methods which are still based on century-old sampling techniques [20].

VI. CONCLUSION

In conclusion, wearable devices are inevitable. They are slowly but surely involving in our everyday life. But there are many questions on the effectiveness and/or the risk of depending on these devices in a large scale. More unanswered questions than answered ones. Will this decrease patient time in clinical settings? Will there be lower re-admittance rates to Emergency Departments? Will it improve overall fitness, nutrition, and wellness? Will it increase security? Will driver/motorcyclist be safer? Will these devices bring us closer to the Singularity?

We’re accustomed to debit and credit cards and purchasing goods over the Internet because they are tied to our bank accounts and net worth plus something more precious, our

trustworthiness. Crypto-currency is a form of digital currency that is available for purchase on exchanges. Like all currencies, it can be used to purchase goods and services where it is accepted but no coins are used. As new concept and a technology under development, crypto-currency introduces new challenges that financial institutions, government and people need to face.

REFERENCES

[1] S. Brostoff and C. Jennett, "Federated identity to access e-government services: are citizens ready for this?". DIM'13, 8-Nov-2013.

[2] "InCommon," [Online]. Available: http://www.incommonfederation.org. [Accessed: 01-Dec-2013].

[3] S. Landau and T. Moore, "Economic tussles in federated identity management," First Monday, vol. 17, no. 10, pp. 1–20, 2012.

[4] "eID Infrastructure for Trustworthy Services in eGovernment and eCommerce" 2012 http://world-comp.org/p2012/SAM9717.pdf.

[5] " Federated Identities: OpenID vs SAML vs OAuth", [Online]. Available: http://www.softwaresecured.com/2013/07/16/federated-identities-openid-vs-saml-vs-oauth. [Accessed: 16-Jan-2014]

[6] E. Ghazizadeh, J. Ab Manan A. Pashang, and M Zamani "A Survey on Security Issues of Federated Identity in the Cloud Computing," IEEE 4th International Conference on Cloud Computing Technology and Science 2012 pp. 562-565

[7] "NIST Releases Second Draft of Federal ID Credential Security Standard for Comment" [Online], http://www.nist.gov/itl/csd/piv-071112.cfm, [Accessed]: 01-Dec-2103www.bitcoin.org, accessed 02/03/2014.

[8[Security without Identification: Transaction Systems to make Big Brother Obsolete, David Chaum, ACM 28 no.10 (Oct 1985), pp. 1034-1044.

[9] Untraceable Electronic Cash, David Chaum, Advances in Cryptology CRYPTO '88, Springer-Verlag, pp. 390-407.

[10] Universal Electronic Cash, Tatsuaki Okamoto, Advances in Cryptology CRYPTO '91, Springer-Verlag, pp. 324-337.

[11] Wallet Databases with Observers, David Chaum, Advances in Cryptology CRYPTO '92, Springer-Verlag, pp. 89-105.

[12] The Cryptography of Anonymous Electronic Cash, Frank Fried, 1996, http://groups/csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.html accessed 02/11/2014.

[13] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, 2009, www.bitcoin.org/bitcoin.pdf accessed 2/13/2014.

[14] Blind signatures for untraceable payments, David Chaum, Advances in Cryptology Proceedings of Crypto, pp 199-203, 1982.J. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility (Periodical style)," *IEEE Trans. Electron Devices*, vol. ED-11, pp. 34–39, Jan. 1959.

[15] *What is Telemedicine*, American Telemedicine association - http://www.americantelemed.org/about-telemedicine/what-is-telemedicine.

[16] M. Kaku, *Physics of the Future*, Doubleday Books, 2011.

[17] N. Agoulmine, M. J. Deen, J. Lee, and M. Meyyappan, *U-Health Smart Home*. IEEE Nanotechnology Magazine, 2011

[18] J. Dudley, Dudley Lab. http://dudleylab.org/

[19] L. Mearian, *World's data to grow 50-folds by 2020*. IDC, 2011.

[20] V. Mayer-Schonberg, K. Cukier, Big Data: A Revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt, 2013.

[21] Baldwin, Roberto. "Google glasses face serious hurdles, augmented-reality experts say." Wired (2012).

[22] Narayanaswami, Chandra, and Mandayam T. Raghunath. "Application design for a smart watch with a high resolution display." 2012 16th International Symposium on Wearable Computers. IEEE Computer Society, 2000.

[23] Airy, James F., and Thomas D. Kadavy. "Wearable apparatus for exercising body joints." U.S. Patent No. 4,801,138. 31 Jan. 1989.

[24] Al-Muhtadi, Jalal, Dennis Mickunas, and Roy Campbell. "Wearable security services." Distributed Computing Systems Workshop, 2001 International Conference on. IEEE, 2001.