IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON CYBER-THREATS AND COUNTERMEASURES IN THE HEALTHCARE SECTOR

Received March 28, 2018, accepted April 26, 2018, date of publication May 7, 2018, date of current version June 5, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2833509

Preparing for Secure Wireless Medical Environment in 2050: A Vision

MUHAMMAD IMRAN MALIK[1], IAN MCATEER[1], (Student Member, IEEE), PETER HANNAY[2], AND ZUBAIR BAIG[3], (Member, IEEE)

[1]School of Science, Edith Cowan University, Joondalup, WA 6027, Australia
[2]Asterisk Information Security and School of Science, Edith Cowan University, Joondalup, WA 6027, Australia
[3]Data61, CSIRO, Melbourne, VIC 3008, Australia

Corresponding author: Muhammad Imran Malik (mimalik@our.ecu.edu.au)

ABSTRACT The world is on the verge of a technological evolution that will revolutionize Internet access across the globe using direct device-to-satellite links. Such direct global connectivity brings with it an opportunity for the medical community to have a new framework for the secure transmission of confidential personal medical information and clinical systems data. Such a framework has the potential to connect developed-country expertise with less-advanced health services in developing countries, remote communities, patients' homes, or in disaster zones. This paper explores this emerging concept along with potential communication advancements in medical equipment and presents a conceptual view of implementing ever-demanding health-care services that can benefit the global population. Further, the paper elaborates upon cyber security challenges to digital health-care services. We provide evidence on the need to improve or develop encryption and hashing algorithms and how it can help to meet the cyber security challenges faced by key stakeholders for e-Health. This will ensure fast, reliable, and effective health-care services for both developing economies and remote locations in developed countries.

INDEX TERMS Secure transmission of medical data, direct satellite communications, encryption, quantum cryptography, solar power, battery/storage cell technology, cyber security.

I. INTRODUCTION

Before the modern/information age, reliable and efficient public healthcare systems were judged on professionalism, the skill of their practitioners and strict administrative controls. In those days, healthcare systems were mainly meant to provide a front-line defense against communicable diseases or pandemics for the patients, facilitate medical research along with innovation and were also aimed at delivering therapeutic outcomes [1]. However, recent technical advances have witnessed the spread of communication networks across the globe which has brought substantial improvements in telecommunication infrastructure and computing technologies which have led to the digitization of personal health information. Not only this, the increase in interconnectivity between medical devices and other clinical systems is also on the rise [2]. Such developments have added another facet in ascertaining a reliable health care system, i.e. how to secure digitized personal health information of an individual. Tomossy *et al*. [1] argue that while digital data assists healthcare providers in instant access to consolidated health records, such systems are prone to significant breaches of privacy and jeopardizes the relationship between doctor and patient. Therefore, personal information has become a treasured commodity, and attackers are always looking for means and ways to steal it [3]. However, adoption of a layered security model can help in mitigating this hyper-evolving threat landscape in the cyber world [4].

Quality health-care is still something that can only be imagined in developing countries [5]. A similar situation also exists in remote/rural areas of developed countries as well. Despite the fact that Governments designate a major chunk of their economy on health-care infrastructure, provision of similar treatment to all of its citizens is not possible due to number factors that include hospitals in rural areas, moving doctors to such areas or bringing patients to urban centers. On the other hand, significant improvements in technology such as the use of wireless mobile devices have enabled patients to be aware of their diagnostic status, disease control, and monitoring as they can move along with such devices easily. Global Internet access using direct communications with low-earth-orbit satellites is the latest technological invention, unlike previous satellite systems dependent on

ground control stations, that many major vendors are looking to explore. Once successfully tested, this concept is expected to change the scenario of human thinking. Access to the Internet using this media will enable remote areas being connected to the rest of the world which otherwise appears impossible. The National Research Council [6] argues that there exist two foremost drivers that will compel Governments and health-care providers to embrace this change. These drivers are the low cost of care, and the fact that health-care delivered at home is valued by patients which in turn promote healthy living and well-being [6].

This paper frames the aforementioned intricate problem of provision of health-care services in areas where such services are difficult to be provided or maintained. The paper also discusses the conjecture that medical equipment will become increasingly deployed in patients' homes and remote areas. Implementation of Internet access using satellites will also see these units becoming more portable and having increased capabilities. In urban areas, this will result in less demand for hospital beds and a decrease in demand for outpatient facilities. Although considered essential regarding reliability, efficiency, availability, and comfort, the need to minimise the potential impact of security breaches and to have strong encryption mechanisms while data is at rest and moving is presented.

II. RESEARCH OBJECTIVES

The objective of this research is to propose practical frameworks (primary and secondary) for the secure and robust exchange of medical information without compromising data integrity particularly when medical devices are used in homes and rural communities. The investigation aims to achieve following objectives:

1) Effective use of the latest technology trends to help reach medical facilities to patients' homes/rural communities.
2) Secure exchange of personal medical information.
3) Use of secure encryption algorithms purely for the medical community.
4) Assist Governments in reducing their expenses on developing hospitals/out-patient facilities.
5) Help the developing countries in utilising the latest technology trends to access developed countries expertise.
6) Non-reliance on patients' modem/router used for normal Internet surfing.

III. BACKGROUND INFORMATION

A. GLOBAL SATELLITE COMMUNICATIONS (THE FUTURE OF INTERNET COMMUNICATION)

On 28 April 2016, OneWeb applied to the U.S. Federal Communications Commission (FCC) proposing the implementation of global high-speed Internet coverage using a constellation of low earth orbit (LEO) satellites [7] to provide global 100Mbps-1Gbps Internet coverage. In response, the FCC asked companies proposing similar systems to declare themselves by 15 November 2016 [8]. A further eleven proposals were received on this date, containing differing ideas on how the satellites would be deployed. Non-geostationary earth orbit (NGSO), inclined geosynchronous earth orbit (IGSO), very low earth orbit (VLEO), low earth orbit (LEO), medium earth orbit (MEO), highly-elliptical orbit (HEO); and utilising polar, inclined or equatorial planes [9] denote differing methodologies. These twelve FCC applications are listed below:

1) Audacy [10] - 3 satellite relays in MEO to communicate with LEO spacecraft.
2) Boeing [11] - 60 IGSO satellites (this is separate from the smallsat filing they also have).
3) Karousel [12] - 12 IGSO satellites for video.
4) Kepler MULTUS [13] - 2-140 LEO nanosats for M2M communication.
5) LeoSat [14] - 78 satellites in LEO.
6) O3b Networks [15] - Amendment to add another 40 satellites.
7) OneWeb [16] - 720 satellites in LEO.
8) Space Norway [17] - 2 satellites in high-inclination 16-hour orbit.
9) SpaceX [18] - 4425 NGSO satellites in LEO.
10) Telesat Canada [19] - 117 satellites in LEO.
11) Theia Holdings [20] - 112 satellites for remote sensing.
12) ViaSat [21] - 24 satellites in polar MEO.

The majority of these applications relate to proposed operations in the Ku-Band and Ka-Band frequency ranges (typically 10.70-12.70 GHz downlink/12.75-14.50 GHz uplink and 17.80-20.20 GHz downlink/27.50-30.00 GHz uplink respectively) [22]. On 1 March 2017, the FCC received seven amendments and additions to some of the previous applications to seek licenses to operate on V-Band frequencies (typically 37.50-42.50 GHz downlink/47.20-52.40 GHz uplink) as well [23]. These seven applications are listed below:

1) Boeing [24] - Amendment to reduce orbit on 2016 V-Band application.
2) Boeing [25] - Application for 2017 V-Band NGSO FSS system.
3) O3b Networks [26] - Amendment to add V-Band spectrum.
4) OneWeb [27] - Application for 2017 V-Band NGSO FSS system.
5) SpaceX [28] - Application for 2017 V-Band NGSO FSS system.
6) Telesat Canada [29] - Letter of Intent to provide service in the US (V-Band).
7) Theia Holdings [30] - Amendment to add V-Band spectrum.

While it is unlikely that all of these FCC applications will be successful, several of the bigger players (for example, SpaceX and OneWeb) have commenced construction of supporting infrastructure and have set preliminary timeframes for

the launching of satellites for testing purposes. OneWeb has commenced construction of a satellite manufacturing facility in Exploration Park, Florida [31], while SpaceX took over approximately 2,800 m2 facility in Redmond, Washington, in 2014 for its communications center [32]. SpaceX recently added to this by procuring a second 3,800 m2 (approximately) facility nearby for satellite development [33].

OneWeb intends an initial launch of 10 satellites using a 'Europeanized Russian Soyuz' rocket in May 2018 [34]. Following to this, the company plans to launch a constellation of 648 satellites (40 SVs in 18 orbital planes) at an altitude of 1200 km in a bid to have a fully operational system by 2027 [35]. As their website states, their goal is "To fully bridge the Digital Divide by 2027, making Internet access available and affordable for everyone" [36]. SpaceX suggests 2019 as when they would be ready to commence launches and have a fully operational system by 2024 [37]. Brodkin [38] claims that SpaceX has a plan to launch 4425 satellites at altitudes of 1150-1300 km by 2030. On the other hand, Boeing is also not far behind the companies stated earlier as they plan an initial launch of 1396 satellites at an altitude of 1200 km, to be followed later by an additional 1560 satellites [39].

If OneWeb, SpaceX and Boeing are indicating this timescale to become operational, for this paper, it can, therefore, be assumed that between 2030-2050 global Gigabit Wi-Fi communications will be already established and have become commonplace. Strong competition can be envisaged that will surely lead to reliable, efficient, and high-speed services considering the number of proposals received, and the launch plans of the global satellite companies stated earlier. This framework is therefore considered to have the potential to provide a secure medium for the worldwide transmission of confidential medical data from a patient's home, from remote locations or from anywhere in developing countries direct to developed countries medical facilities. However, the planning of the correct steps particularly by the Governments and health-care providers towards achieving a secure data transmission framework such as this needs to be taken now.

B. GROWING WORLD POPULATION

According to worldmeters [40], the current population of the world at this time of writing now exceeds 7 billion and is currently increasing at a rate of approximately 30 million per year. By 2050, the world population is anticipated to be approaching 10 billion as shown graphically in Figure 1 [41].

It is anticipated that this will have many significant effects, two of which are:

1) Increasing difficulty in feeding the world's population as a whole [42].
2) There will be inadequate infrastructure (hospitals) to cope with all those requiring medical attention as resources available are not directly proportional to the population increase [43].

The above conjecture depicts that huge expenses would be required regarding infrastructure for medical

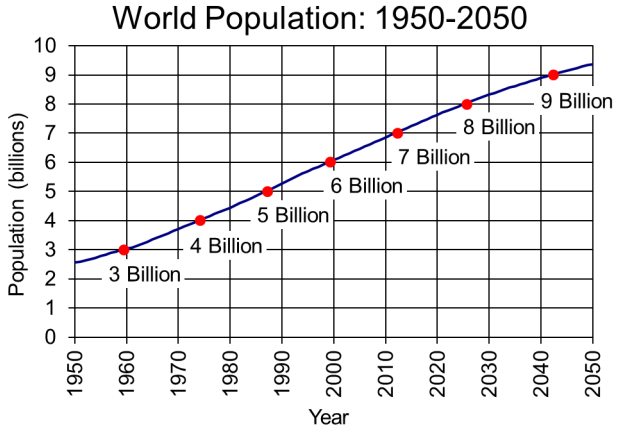


FIGURE 1. World population growth 1950-2050 [41].

equipment/facilities to support such a population. Consequently, this situation poses extreme difficulties not only for developing countries but the developed countries would also be needing huge expenses which are difficult to manage under prevailing economic conditions. This problem is compelling decision-makers to migrate health-care services towards homes and rural areas for a variety of reasons, some of them are [6]:

1) Increased cost in the provision of health-care.
2) Increased number of ageing adults.
3) The rise of chronic disease cases.
4) A wide range of technological innovations.

IV. DISCUSSION

Manyika and Roxburgh [44] claim that digital transformation has altogether changed the way humans work, socialize, exchange information and ideas around the globe. The growing dependence on technology, in particular, the mobile networked technology, has allowed decision-makers such as Governments, health-care providers and other interested parties to embrace the opportunities such systems provide. The emergence of the 'Global Internet' discussed earlier is a recent example in this regard. On the other hand, considering the advances in medical equipment over the past 33 years (since 1984) to assess what might be feasible within the next 33 years gives us a clear understanding how fast humans are progressing to bring ease into their lives. It can, therefore, be envisaged that real-time remote monitoring of an expanding range of medical devices and device instrument-testing/calibration will become feasible beyond what currently exists for cardiovascular implantable electronic devices [45], drug pumps, defibrillators, and neurostimulators [2].

A. IMPROVEMENTS IN COMMUNICATION AND POWER SUPPLY MECHANISMS

It can be envisioned that medical equipment will gradually evolve into autonomous and portable units, with independent

communication mechanisms, i.e. medical equipment being able to communicate directly via satellite Internet services. The world has already seen small handheld devices being able to have direct satellite communication voice/text functions such as Thuraya portable devices [46]. Furthermore, in making medical equipment completely autonomous, such devices also need to be self-sufficient regarding power capabilities, so that they are not reliant on the local grid power supply or generators provided locally or transported to the remote locations. Medical units of the future used in homes and deployed in remote areas or disaster zones should have an independent electrical power supply that is adequate and reliable, that will essentially ensure that data integrity and the transmission of 'live' medical data will not be interrupted by power blackouts. Independent power abilities would also be vital in the field of disaster relief, where local infrastructure would likely be devastated. Advances in the following three areas should make this a feasible goal.

1) IMPROVEMENTS IN SOLAR TECHNOLOGY

Human beings have been exploiting solar energy for thousands of years to meet their daily needs albeit on an individual basis. However, the efficiency of solar panel technology (i.e. how much of the sun's energy is turned into electricity) has steadily advanced in recent years, and the current world record stands at 26.6% [47]. The world has already seen a practical implementation of solar technology, for example, solar-powered watches, which will gradually expand to larger devices such as laptops, etc. It is reasonable to assume that this trend will continue for years to come. Phillips [48] argues that use of solar technology will not only increase efficiency, but this will be aided by the introduction of new materials and technologies. Significant research has moved away from silicon-based materials and is investigating new materials such as perovskite, a calcium titanium oxide mineral [49]. Other aspects of solar-cell research are looking at moving away from the standard solar panel available today, such as investigating flexible films [50] and even spray-on technology [51] which expands the potential applications for solar-powered devices.

2) IMPROVEMENTS IN BATTERY/STORAGE CELL TECHNOLOGY

In recent years the majority of research into rechargeable technology has concerned lithium-based batteries, and this continues today [52]. The electric-car industry is expected to significantly increase demand for this element [53], but there are some concerns whether available resources will be able to meet demand [54]. Non-lithium-based battery research encompasses such technologies as sodium-nickel chloride [55], otherwise known as ZEBRA batteries, and aluminium ion [56]. On the other hand, graphene, a "wonder material" with remarkable properties and potentially an almost endless list of applications [57], is likely to play an increasingly important role in technology in years to come. Graphene-coated electrodes in conventional lithium-ion batteries have significantly enhanced performance [58], [59] and in itself has the feasibility for greatly enhanced performance supercapacitors to be manufactured [59].

3) IMPROVEMENTS IN ENERGY CONSUMPTION FOR DEVICES

Using energy more efficiently is a key strategy while using data processing and communication devices. Such design concerns have become more significant for mobile devices as the demand for 24/7 connectivity combined with the convenience of portability increases. Advances in operational time per charge cycle for devices do not only come from improved battery technology providing long-lasting power, but also from improvements in device design being able to perform the same functions with reduced power consumption. Cullen and Allwood [60] cite in the 'International Energy Agency's World Energy Outlook 2006' by forecasting that the global average energy intensity (a measure of global energy efficiency) will decrease by an average approximately 1.7% per year between 2004 and 2030. The authors went on to say that by 2050 this will equate to energy savings of approximately 55%. In other words, based on current trends and research being conducted, electronic devices are expected to be greatly more efficient regarding power consumption by 2050 compared to the devices today. The potential is, therefore, that fully autonomous medical devices will be even more likely. Not only will solar and storage cell technology improve significantly, but also the amount of electrical energy needed to power such devices will decrease.

B. POSITIVE IMPACTS

Through the above-stated arguments on improvements in various domains, it can be envisaged that greater focus will be placed on having more advanced medical equipment in the home as well as in remote communities. Far-reaching positive impacts of this will be as follows:

1) Moving essential/basic medical equipment from the hospitals to patients' homes/remote communities will reduce demand for hospital beds and outpatient facilities.
2) Patients will be less exposed to secondary infection from other patients in the hospital, and they will also feel less stressed by remaining in familiar surroundings.
3) Reduce demand for patients to travel to get treatment, potentially over long distances from remote communities to urban centers.
4) Availability of more advanced medical equipment helping in disaster-relief efforts.

V. PROPOSED FRAMEWORKS

This section discusses the two frameworks the authors are proposing to provide efficient health-care facilities to patients at home and in remote communities. The primary framework is considered to be an innovative solution and is expected to

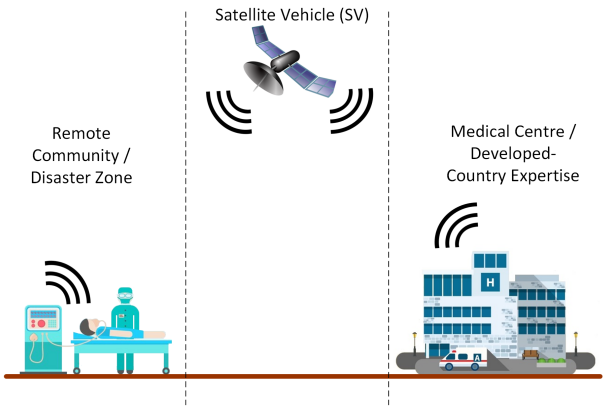


FIGURE 2. Direct satellite transmission from medical equipment to medical centre.

be robust and reliable. However, as the availability of healthcare facilities is considered as the key component to handle the critical cases amicably, a secondary framework has also been proposed.

A. PRIMARY FRAMEWORK

Based on the technological advancements discussed earlier, it can easily be projected that the new space-race into providing global gigabit Wi-Fi connectivity will surely provide a primary framework for the transmission of medical data between each medical device located anywhere in the world, medical centers and at homes. Because OneWeb, SpaceX and Boeing, to name but three, are each planning to launch their global satellites gives a fair indication that this rivalry will provide a more robust and reliable solution for consistent improvement. Furthermore, if medical equipment of the future is to utilize this proposed primary transmission framework, each medical unit needs to have the inbuilt capability of communicating directly with the satellite vehicles (SVs) in orbit. An illustration of how such system will look like when deployed in a rural community center is presented in Figure 2.

Figure 2 shows how medical data will be sent from and received by medical equipment or a clinical system situated in a rural community center and operated by paramedical staff. This data is transported using satellite vehicle(s) to a professional doctor or a surgeon in an urban medical centre or a hospital for analysis and subsequent advice. The same illustration is also true in a situation where a person living in a developing country is looking for advice from a professional in a developed country.

Though it is assumed that this new technology will be steadfast keeping in view the giant companies involved and the significant investments being made by them, total reliance on satellite communications for the secure transmission of medical data is unwise. It can be attributed to the research undertaken by Dehling and Sunyaev [61] that availability of medical services is vital for the information security triad. The proposed primary framework could, therefore, be compromised by:

1) A technical malfunction within the satellite in orbit [62] or at a ground control station [63].
2) Being more prone to cyber-attacks [64].
3) The impact from space junk [65].
4) Solar storms from coronal mass ejections, particularly at the peaks of the 12-yearly sunspot cycle [66].

B. SECONDARY FRAMEWORK

Based on the factors related to the availability of global satellites as explained earlier, it is considered necessary to build redundancy into the communications system by providing a secondary backup framework. Williams and Woodward [2] argue that having a redundant system ensures that failure of one (primary) system does not affect the availability of a service. Particular to the problem being addressed through this research, a secondary transmission framework will need to utilize whatever terrestrial methods of communication are available. If the aim of being able to deploy medical equipment in various settings is to be achieved, this framework needs to be multi-faceted to enable connection via such media as fiber-optic cable or Wide Area Network (WAN) wireless connections. Medical equipment also needs to have the appropriate modem/router and connections to enable connectivity to whatever type of network access is available at the site of deployment. Modems/routers could be either inbuilt or come as a peripheral device shipped with the medical unit. However, the authors believe that such devices should be inbuilt to the medical units as this will ensure ease of management and overcome the requirement of having multiple power sources.

VI. CYBER SECURITY CHALLENGES

It is worth mentioning that the current value of credit card information for a single card on the dark web black market is less than US$0.20 when purchased in bulk [67]. However, the current value of electronic medical information for one individual on the dark web black market is approximately US$20 which is used for identity theft and possibly to launch more attacks [68]. It has, therefore, become essential to protect the privacy and confidentiality to overcome identity theft attacks. The need to ensure confidentiality, integrity, and availability of medical data while being transmitted or at rest via the proposed frameworks, in particular, the primary framework, requires a review and modification of existing standards and policies. The recent ransomware attack 'WannaCry' that attacked UK's National Health Service (NHS) [69] speaks of weak standards, policies and poor implementation of security controls. Therefore, having sufficient and well-planned security controls become more significant as moving medical equipment to patients' homes/remote communities will require a greater focus on the secure exchange of personal information to the hospital/doctor to keep the privacy of a patient's personal information from being compromised. Effective coordination between security and medical professionals to make the latter realise and understand the

importance of information security through awareness programs is required [70].

Current hand-held technology is capable of direct voice/text communications via satellite. As discussed so far in this paper, by 2050 it is reasonable to expect medical equipment to be able to communicate directly to satellites in a similar fashion. Thus, hardware needs to be embedded with appropriate secure communication mechanisms to be wholly independent of patients' or remote communities' Wi-Fi access, IoTs, etc. and encrypt the medical data to prevent loss of confidentiality or integrity. Isolation from home-users' modems is important since these are normally considered highly insecure [71].

A simplified form of Moore's Law, derived by Gordon E. Moore in 1965, states that processor speed will double approximately every two years [72]. However, in recent years this theory has started to break down, as was predicted by Intel's David House in 2005 [73], who suggested 18 months is a more realistic figure. If we assume, therefore, that as a rule of thumb computer power will double every 18 months, then computer power will be approximately $2^{21.33}$ or over 2500 times more powerful at the start of 2050 compared to what it is at the time of writing (early 2018).

The most secure encryption algorithm commercially available today is considered to be RSA-4096 [74]. RSA-4096 relies on the mathematical premise that it is difficult to factor very large numbers. However, Worstall [75] reported that researchers in Israel were able to bypass this in approximately one hour in a proof-of-concept experiment. Future computing power and its potential to render current encryption methods entirely ineffectual are well understood, and the development of new methodologies is also underway. Chen [76] reports that quantum cryptography ''is so powerful because it is physically impossible for a hacker to steal a key encoded using quantum particles''. Chen [76] goes on to say that "the eventual goal is to deliver quantum keys to a satellite, which could make it possible to send quantum-secured messages across the globe". This goal is aligned with the subject of this paper, namely the use of global Wi-Fi frameworks for the secure transmission of medical data and the enabling of secure remote firmware/software updating and calibration. It is clear that encryption algorithms inbuilt into medical devices of the future should be utilizing concepts as proposed by Chen [76] as soon as the global Internet becomes commercially available. The trust level between doctor and patient as stated otherwise earlier will certainly enhance.

A similar situation exists when dealing with available hashing algorithms. In 2004 the Message Digest version 5 (MD5) hash algorithm was broken by collision attack [77]. In February 2017, the Secure Hash Algorithm version 1 (SHA-1) was broken by the same method [78]. Increasing computer power will gradually threaten other hashing algorithms (e.g. SHA-2, SHA-3, SHA-256, SHA-512). Medical equipment manufacturers need to remain vigilant to evolving threats and hackers' capabilities and take mitigating steps to avoid such vulnerabilities developing over time.

It is a well-known fact that health-care providers give patient safety more importance than having to think about cyber security challenges applicable to the modern medical devices in use. For obvious reasons, this will remain the status quo until proper cyber-awareness training is provided to medical staff. The expansion of networked medical devices opens a challenge of controlling cyber security in this arena. Williams and Woodward [2] describe such challenges as follows:

1) Making health-care organisations understand the cyber security vulnerabilities present in the medical devices and making them aware of a security breach and privacy issues.
2) Cyber security protection in the medical devices to be embedded from their conception.
3) Development of relevant cyber security standards that can assist manufacturers and implementers to ensure compliance.
4) Inculcating awareness of cyber security and privacy issues on a regular basis.

VII. CONCLUSIONS AND RECOMMENDATIONS

Medical equipment should become more autonomous due to advancements in medical technology, including new paths of communication (in this case, the global Internet via satellite), and the enhanced efficiency of solar power and batteries/power supplies. These advances will enable remote access to live patient data in patients' homes, or indeed anywhere in the world, from medical centers. Placing medical equipment in patients' homes or remote communities will, in the former case, decrease the demand for outpatient facilities and hospital beds at medical centers, and in the latter, save patients from having to make long-distance travel to urban centres for certain medical treatments. Such deployments will surely assist Governments in reducing their expenses incurred in developing hospitals or out-patient facilities. For patients in developing countries, developed-country expertise can constantly be remotely available in real time. In disaster zones, such as an earthquake or flood-affected area, enhanced medical care without the dependence on shipping heavy generator equipment will become available to those in life-threatening conditions.

Independent lines of data transmission through direct satellite communications will circumvent any dependence on local Wi-Fi or terrestrial network infrastructure outside the confines of medical centres, and therefore health-care services will flourish exponentially since patient safety is paramount over any security issues. The challenge here is to ensure that appropriate cyber security measures are in place to reduce the risks of this multifaceted domain. Various vulnerabilities related to data-in-transit and data-at-rest can be mitigated, such as being able to bypass patients' or remote community network devices which may be infected by malware. Having inbuilt functionality within the medical unit, i.e. modems/routers to communicate through any of the

proposed frameworks, will also ensure non-reliance on patients' modem traditionally used through copper or fiber media for Internet surfing.

Furthermore, failures in securing digital health-care services are well-documented, particularly in wireless communications [2]. While existing standards, policies, and procedures are being updated to accommodate the new primary framework of secure transmission of medical data via low-earth-orbit satellite links; this would be an appropriate time to review and modify shortcomings in current policies related to terrestrial communications.

The requirement of improved or new encryption and hashing algorithms is considered the need of the hour to ensure secure exchange of medical information. A joint consortium of universities with strong research potential, security and health-care professionals, private companies particularly those involved in the launch of global satellite vehicles as well as medical equipment manufacturers, Governments and other health-care providers can effectively achieve this. Furthermore, the major challenge for health-care providers as argued by Williams [70] is to make them understand the importance of information security without hindering their workflow remains a major challenge for which regular security awareness activities need to be undertaken.

VIII. FUTURE WORK

The research undertaken for this paper provides a conceptual view of how the emerging technology can be exploited to accrue maximum benefits while addressing medical needs of every human being as their basic right. The research also draws a theoretical picture of how the security of medical data can be achieved through the proposed frameworks. A whole new avenue for researchers to look into the practical aspects of the proposed frameworks is opened up, with a particular focus on information security triad: confidentiality, integrity, and availability. A few of them are listed as under:

1) An in-depth review of protocols used in global satellite communication from a security perspective.
2) Investigate the possibility of using dedicated satellite channels purely for the secure transmission of medical data.
3) Investigate direct connectivity to satellite and terrestrial frameworks either by inbuilt means within the medical equipment or via external peripheral devices.
4) Investigate the use of advanced and upgradable encryption mechanisms that are fast and also ensures integrity and confidentiality of medical data.
5) Review of past breaches of security concerning medical data to propose improvised policies to encompass existing and future communication frameworks.

REFERENCES

[1] G. F. Tomossy, Z. J. Bending, and P. Maluga, "Privacy and metadata: The hidden threat to whistle-blowers in public health systems," *Ethics, Med. Public Health*, vol. 3, no. 1, pp. 124–133, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2352552517300257

[2] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem," *Med. Devices, Evidence Res.*, vol. 8, pp. 305–316, Jul. 2015. [Online]. Available: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/

[3] J. Banks, "The Heartbleed bug: Insecurity repackaged, rebranded and resold," *Crime, Media, Culture, Int. J.*, vol. 11, no. 3, pp. 259–279, 2015. [Online]. Available: http://journals.sagepub.com/doi/full/10.1177/1741659015592792

[4] J. Scott and D. Spaniel, *Your Life, Repackaged and Resold: The Deep Web Exploitation of Health Sector Breach Victims*. CreateSpace Independent Publishing Platform, 2016. [Online]. Available: https://books.google.com.au/books?id=JEz7MAAACAAJ

[5] K. L. Courtney, O. Shabestari, and A. Kuo, *Enabling Health and Healthcare Through ICT: Available, Tailored and Closer* (Online Access: EBSCO eBook Clinical Collection). Amsterdam, The Netherlands: IOS Press, 2013. [Online]. Available: https://books.google.com.au/books?id=uuZNnyYWK2EC

[6] National Research Council. (2011). *Health Care Comes Home: The Human Factors*. [Online]. Available: http://public.eblib.com/choice/publicfullrecord.aspx?p=3378794

[7] P. B. de Selding. (2016). *OneWeb to Debut as B2B Broadband Wholesaler Before Serving World's Poorest*. [Online]. Available: http://spacenews.com/oneweb-files-for-u-s-license-will-debut-as-b2b-broadband-wholeseller-before-expanding-to-worlds-poorest/

[8] FCC. (2016). *Cut-Off Established For Additional NGSO-Like Satellite Applications*. [Online]. Available: https://apps.fcc.gov/edocs_public/attachmatch/DA-16-804A1.pdf

[9] P. B. de Selding. (2016). *Enough Satellites to Darken the Skies*. [Online]. Available: https://www.spacenewsmag.com/the-bottom-line/enough-satellites-to-darken-the-skies/

[10] FCC. (2016). *Audacy Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOA2016111500117&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[11] FCC. (2016). *Boeing Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOA2016111500109&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[12] FCC. (2016). *Karousel Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOA2016111500113&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[13] FCC. (2016). *Kepler Multus Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOI2016111500114&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[14] FCC. (2016). *Leosat Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOI2016111500112&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[15] FCC. (2016). *O3b Network Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATAMD2016111500116&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[16] FCC. (2016). *Oneweb Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOI2016042800041&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[17] FCC. (2016). *Space Norway Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOI2016111500111&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[18] FCC. (2016). *Spacex Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOA2016111500118&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[19] FCC. (2016). *Telesat Canada Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOI2016111500108&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[20] FCC. (2016). *Theia Holdings Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOA2016111500121&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[21] FCC. (2016). *Viasat Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOI2016111500120&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[22] M. Albulet. (2016). *Spacex Non-Geostationary Satellite System; Attachment A; Technical Information to Supplement Schedules*. [Online]. Available: https://cdn.arstechnica.net/wp-content/uploads/2016/11/spacex-Technical-Attachment.pdf

[23] C. Henry. (2017). *FCC Gets Five new Applications for Non-Geostationary Satellite Constellations*. [Online]. Available: http://spacenews.com/fcc-gets-five-new-applications-for-non-geostationary-satellite-constellations/

[24] FCC. (2017). *Boeing Amendment to Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATAMD2017030100030&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[25] FCC. (2017). *Boeing Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOA2017030100028&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[26] FCC. (2017). *Ob3 Network Amendment to Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATAMD2017030100026&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[27] FCC. (2017). *OneWeb Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOI2017030100031&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[28] FCC. (2017). *Spacex Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOA2017030100027&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[29] FCC. (2017). *Telesat Canada Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATLOI2017030100023&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[30] FCC. (2017). *Theia Holdings Amendment to Petition for Declaratory Ruling*. [Online]. Available: http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/SATAMD2017030100029&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number

[31] OneWeb. (2017). *OneWeb Satellites Breaks Ground on the World's First State-of-the-art High-Volume Satellite Manufacturing Facility*. [Online]. Available: http://oneweb.world/press-releases/2017/oneweb-satellites-breaks-ground-on-the-worlds-first-state-of-the-art-high-volume-satellite-manufacturing-facility

[32] T. Bishop. (2015). *Spacex's new Seattle-Area Office is in Redmond; Elon Musk to Visit Region This Week*,. Available: https://www.geekwire.com/2015/spacexs-new-seattle-area-office-redmond-elon-musk-visit-region-week/

[33] A. Boyle. (2017). *Spacex Adds a Big New Lab to its Satellite Development Operation in Seattle Area*. [Online]. Available: https://www.geekwire.com/2017/spacex-lab-satellite-development-redmond/

[34] Advanced Television. (2017). *OneWeb Plans May 2018 Launch*. [Online]. Available: https://advanced-television.com/2017/10/31/inside-satellite-oneweb-plans-may-2018-launch/

[35] S. Clark. (2015). *OneWeb Selects Airbus to Build 900 Internet Satellites*. [Online]. Available: https://spaceflightnow.com/2015/06/15/oneweb-selects-airbus-to-build-900-internet-satellites/

[36] G. Wyler. (2016). *OneWeb: We all Need Access*. [Online]. Available: http://oneweb.world

[37] R. McCormick. (2017). *SpaceX Plans to Launch First Internet-Providing Satellites in 2019*. [Online]. Available: https://www.theverge.com/2017/5/4/15539934/spacex-satellite-internet-launch-2019

[38] J. Brodkin. (2016). *SpaceX Plans Worldwide Satellite Internet With Low Latency, Gigabit Speed*. [Online]. Available: https://arstechnica.com/information-technology/2016/11/spacex-plans-worldwide-satellite-internet-with-low-latency-gigabit-speed/

[39] A. Boyle. (2016). *5G or not 5G? Boeing Joins the Battle Over Broadband Satellite Spectrum*. [Online]. Available: http://www.geekwire.com/2016/boeing-battle-broadband-internet-satellite/

[40] Worldometers. (2017). *Current World Population*. [Online]. Available: http://www.worldometers.info/world-population/

[41] U.S. Census Bureau. (2016). *World Population: 1950–2050*. [Online]. Available: https://www.census.gov/population/international/data/worldpop/graph_population.php

[42] L. Kehoe. (2016). *Comment: Can We Feed a Growing World Population and Also Stop Deforestation?* [Online]. Available: http://www.sbs.com.au/news/article/2016/04/20/comment-can-we-feed-growing-world-population-and-also-stop-deforestation

[43] Nuffield Trust. (2014). *New Analysis Reveals Scale of Future Pressure on Hospital Beds*. [Online]. Available: https://www.nuffieldtrust.org.uk/news-item/new-analysis-reveals-scale-of-future-pressure-on-hospital-beds

[44] J. Manyika and C. Roxburgh. (2011). *The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity*. [Online]. Available: http://www.mckinsey.com/industries/high-tech/our-insights/the-great-transformer

[45] B. Wilsmore and J. Leitch, "Remote monitoring of medical devices in Australia," *The Med. J. Austral.*, vol. 206, no. 2, pp. 62–63, 2017. [Online]. Available: https://www.mja.com.au/journal/2017/206/2/remote-monitoring-medical-devices-australia?0=ip_login_no_cache%3D79f0c9f4e51774a2941b6bac2531afed

[46] Thuraya. (2017). *Products List*. [Online]. Available: http://www.thuraya.com/products-list

[47] D. Nield. (2017). *Scientists Have Broken the Efficiency Record for Mass-Produced Solar Panels*. [Online]. Available: http://www.sciencealert.com/researchers-have-broken-the-record-for-solar-panel-efficiency-again

[48] L. Phillips. (2016). *The Future of Solar Power Technology is Bright*. [Online]. Available: https://arstechnica.com/science/2017/02/for-a-brighter-future-science-looks-to-re-energize-the-common-solar-cell/

[49] J.-P. Correa-Baena *et al.*, "The rapid evolution of highly efficient perovskite solar cells," *Energy Environ. Sci.*, vol. 10, no. 3, pp. 710–727, 2017.

[50] M. Hála *et al.*, "Improved environmental stability of highly conductive nominally undoped ZnO layers suitable for n-type windows in thin film solar cells," *Solar Energy Mater. Solar Cells*, vol. 161, pp. 232–239, Mar. 2017. [Online]. Available: http://ac.els-cdn.com/S0927024816304871/1-s2.0-S0927024816304871-main.pdf?_tid=a683d29e-39f6-11e7-add9-00000aab0f02&acdnat=1494911897_23b11ca9de9bcd7c7ae5343c9bfc29c2

[51] M. Eslamian, "Inorganic and organic solution-processed thin film devices," *Nano-Micro Lett.*, vol. 9, p. 3, Jan. 2017. [Online]. Available: https://link.springer.com/article/10.1007/s40820-016-0106-4

[52] C. Sun, J. Liu, Y. Gong, D. P. Wilkinson, and J. Zhang, "Recent advances in all-solid-state rechargeable lithium batteries" *Nano Energy*, vol. 33, pp. 363–386, Mar. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2211285517300356

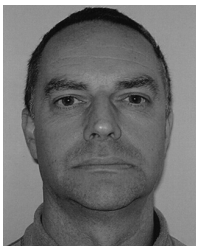
[53] S. Freeman. (2017). *Lithium is the Latest Hot Metal Commodity, but Investor Fever Could be Cooling*. [Online]. Available: http://business.financialpost.com/news/mining/lithium-is-the-latest-hot-metal-commodity-but-investor-fever-could-be-cooling

[54] T. Hunt. (2015). *Is There Enough Lithium to Maintain the Growth of the Lithium-Ion Battery Market?* [Online]. Available: https://www.greentechmedia.com/articles/read/Is-There-Enough-Lithium-to-Maintain-the-Growth-of-the-Lithium-Ion-Battery-M

[55] O. Veneri, C. Capasso, and S. Patalano, "Experimental study on the performance of a ZEBRA battery based propulsion system for urban commercial vehicles," *Appl. Energy*, vol. 185, pp. 2005–2018, Jan. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S030626191630112X

[56] Y. Gao, C. Zhu, Z. Chen, and G. Lu, "Understanding ultrafast rechargeable aluminum-ion battery from first-principles," *J. Phys. Chem. C*, vol. 121, no. 13, pp. 7131–7138, 2017. [Online]. Available: http://pubs.acs.org/doi/abs/10.1021/acs.jpcc.7b00888
[57] University of Manchester. (2014). *The Applications*. [Online]. Available: http://www.graphene.manchester.ac.uk/explore/the-applications/
[58] Y. Li, J. Yang, and J. Song, "Nano energy system model and nanoscale effect of graphene battery in renewable energy electric vehicle," *Renew. Sustain. Energy Rev.*, vol. 69, pp. 652–663, Mar. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S136403211630884X
[59] University of Manchester. (2014). *Energy*. [Online]. Available: http://www.graphene.manchester.ac.uk/explore/the-applications/energy/
[60] J. M. Cullen and J. M. Allwood, "The efficient use of energy: Tracing the global flow of energy from fuel to service," *Energy Policy*, vol. 38, no. 1, pp. 75–81, 2010. [Online]. Available: https://EconPapers.repec.org/RePEc:eee:enepol:v:38:y:2010:i:1:p:75-81
[61] T. Dehling and A. Sunyaev, "Information security and privacy of patient-centered health it services: What needs to be done?" in *Proc. 47th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2014, pp. 2984–2993.
[62] T. Malik. (2011). *Canadian Satellite Malfunction Leaves Thousands Without Communications*. [Online]. Available: http://www.space.com/13213-canadian-communications-satellite-malfunctions-anik-f2.html
[63] M. Kramer. (2013). *Space Station Loses Contact With NASA Mission Control*. [Online]. Available: http://www.space.com/19853-space-station-contact-lost-nasa.html
[64] A. Newcomb. (2016). *Hacked in Space: Are Satellites the Next Cybersecurity Battleground?*. [Online]. Available: http://www.nbcnews.com/storyline/hacking-in-america/hacked-space-are-satellites-next-cybersecurity-battleground-n658231
[65] E. Hall. (2016). *Space Junk Poses Threat to Navigation and Communication Satellites*. [Online]. Available: http://www.abc.net.au/worldtoday/content/2016/s4472628.htm
[66] S. Anthony. (2014). *The Solar Storm of 2012 That Almost Sent us Back to a Post-Apocalyptic Stone Age*. [Online]. Available: https://www.extremetech.com/extreme/186805-the-solar-storm-of-2012-that-almost-sent-us-back-to-a-post-apocalyptic-stone-age
[67] L. Grilli. (2017). *A Look at What's Happening With Stolen Card Cata, Credentials*. [Online]. Available: http://www.cutoday.info/Fresh-Today/A-Look-At-What-s-Happening-With-Stolen-Card-Data-Credentials
[68] A. Espinosa. (2017). *Study Details the Value of Stolen Medical Records*. [Online]. Available: http://onlinesecurity.trendmicro.com.au/study-details-the-value-of-stolen-medical-records/
[69] D. Gayle, A. Topping, I. Sample, S. Marsh, and V. Dodd. (2017). *NHS Seeks to Recover From Global Cyber-Attack as Security Concerns Resurface*. [Online]. Available: https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack
[70] P. A. H. Williams. (2011). *Help or Hindrance: The Practicality of Applying Security Standards in Healthcare*. [Online]. Available: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1131&context=ism
[71] T. Stimpson, L. Liu, J. Zhang, R. Hill, W. Liu, and Y. Zhan, "Assessment of security and vulnerability of home wireless networks," in *Proc. 9th Int. Conf. Fuzzy Syst. Knowl. Discovery (FSKD)*, May 2012, pp. 2133–2137.
[72] The Editors of Encyclopdia Britannica. (2017). *Moore's Law*. [Online]. Available: https://www.britannica.com/topic/Moores-law
[73] M. Peckham. (2012). *The Collapse of Moore's law: Physicist Says its Already Happening*. [Online]. Available: http://techland.time.com/2012/05/01/the-collapse-of-moores-law-physicist-says-its-already-happening/
[74] R. Tripathi and S. Agrawal, "Comparative study of symmetric and asymmetric cryptography techniques," *Int. J. Adv. Found. Res. Comput.*, vol. 1, no. 6, pp. 68–76, 2014. [Online]. Available: http://www.ijafrc.org/Volumn1/Vol_issue6/9.pdf
[75] T. Worstall. (2013). *Researchers Break RSA 4096 Encryption With Just a Microphone and a Couple of Emails*. [Online]. Available: https://www.forbes.com/sites/timworstall/2013/12/21/researchers-break-rsa-4096-encryption-with-just-a-microphone-and-a-couple-of-emails/#7da30fb52181
[76] S. Chen. (2017). *Physicists, Lasers, and an Airplane: Taking Aim at Quantum Cryptography*. [Online]. Available: https://www.wired.com/2017/02/physicists-test-quantum-cryptography-playing-catch-photons-plane/
[77] D. Kaminsky. (2004). *Md5 Message Digest Algorithm Hash Collision Weakness*. [Online]. Available: http://www.securityfocus.com/bid/11849/discuss
[78] D. Goodin. (2017). *Watershed Sha1 Collision Just Broke the Webkit Repository, Others may Follow*. [Online]. Available: https://arstechnica.com/security/2017/02/watershed-sha1-collision-just-broke-the-webkit-repository-others-may-follow/

MUHAMMAD IMRAN MALIK received the master's degree in cyber security from Edith Cowan University (ECU) in 2017 and the master's degrees in computer science and networks and telecommunication in 2003 and 2012, respectively. He is currently pursuing the Ph.D. degree in cyber security with the School of Science, ECU. He has over 15 years of industry experience and his research areas include cyber-security, machine learning, smart systems, and malware analysis.



IAN MCATEER is currently pursuing the master's degree in cyber security with the School of Science, Edith Cowan University (ECU). He is currently a Research Assistant with the ECU Security Research Institute. His research areas include cyber-security, IoTs, steganography, and biometrics. In addition, he has a wealth of experience in the seismic industry ranging over 35 years.

PETER HANNAY is currently a Senior Security Consultant with Asterisk Information Security and also an Adjunct Lecturer with the School of Science, Edith Cowan University. He has a significant research background in cyber-security, with a particular focus in the locational history of embedded devices. He has spoken at major industry and academic conferences, both international and domestic.

ZUBAIR BAIG is currently a Senior Research Scientist in cyber security with Data61, CSIRO, Melbourne, Australia. He is also an Adjunct Senior Lecturer with the School of Science, Edith Cowan University. He has authored or co-authored over 60 journal and conference articles and book chapters. His research interests are in the areas of cyber security, artificial intelligence, and optimization algorithms. He is serving as an Editor of the *IET Wireless Sensor Systems* and PSU, a review journal. He has served on numerous technical program committees of international conferences and has delivered several keynote talks on cyber security.