EAI Endorsed Transactions
on Smart Cities

Research Article EAI.EU

Consociate Healthcare System through Biometric Based Internet of Medical Things (BBIOMT) Approach

Sherin Zafar[1,*], Samia Khan[1], Nida Iftekhar[1] and Siddharta Sankar Biswas[1]

[1]Department of CSE, SEST, Jamia Hamdard, India

Abstract

Internet of Medical Things (IOMT) or healthcare Internet of Thing (IOT) is a collection of medical devices and applications that connect the various healthcare systems based on IT through online computer networks. The devices are connected the output Wi-Fi allowing the M-M (machine to machine) communication through IOMT. IOMT provides various applications including remote patient monitoring (RPM), wearable fitness bands (WFB), hospital beds that are sensor equipped and many-more. IOMT allows communication of medical devices without the intervention of human. The widespread deployment of IOMT faces challenges of security, privacy, connectivity as well as compatibility. IOMT based systems suffer from various security breaches and hacking attacks. Traditional security measures of login/password do not compliment IOT based systems. So this research chapter proposes a novel Biometric Based Internet of Medical Things (BBIOMT) technology that is unique and spoof free. The BBIOMT approach eliminates shortcomings of traditional password schemes and offer a much superior authentication solution.

Keywords: IOMT, IOT, BBIOMT

Received on 30 January 2020, accepted on 21 May 2020, published on 23 June 2020

doi: 10.4108/eai.23-6-2020.165499

*Corresponding author. Email: Zafarsherin@gmail.com

1. Introduction

Enabling interaction of machine to machine and intervention of real time solutions to radically transform the delivery, affordability and reliability of healthcare in near future is the basic task of Internet of Medical Things (IOMT). Due to increased engagement of patients in decision making or boosting compliance of healthcare service, leads to increase in technology adoption rate that will reach to about $156 billion by year 2020. Figure.1 depicts utilization of IOMT devices and services currently and in near future (Anya, O., & Tawfik, H, 2016)

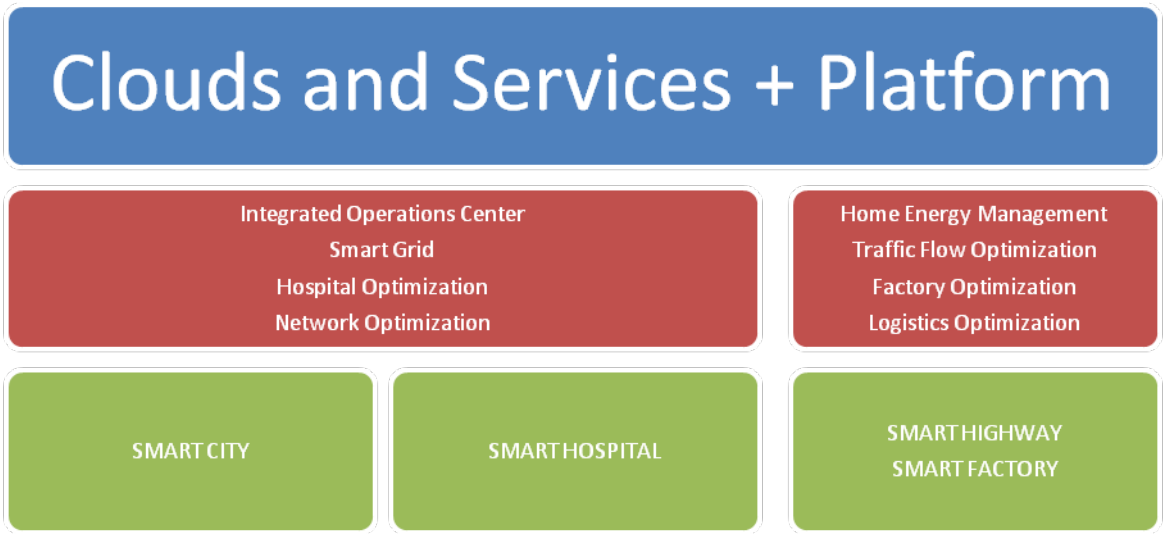


Figure 1. IOMT Devices and Services

IOMT evolved from Internet of Things (IoT) having a complex architecture where multiple components keep on interacting, enabling in providing solutions for the end user. IOT is an interdependent system enabling real time data acquisition connectivity of devices, transfer of data and different analytics for controlling applications of end-user. A connected environment of cyber physical systems integrating data driven human and computer intervention that facilitates decision process is the basic workflow of IOT. Various technologies encompassed by IOT are:

- Smart Grids
- Intelligent Logistics
- Smart towns
- Integration of Data Analytics and Sensors

All the above technologies are augmented by:

- Actuators
- Communication Protocol Networks

The various industry segments where IOT is being utilized and will cause transformation in near future are:

- Manufacturing Industry
- Construction Industry
- Power Distribution
- Healthcare

IOMT is the healthcare application provided by IOT that develops a network comprising of real time sensing of vital data by connected devices. IOMT lead to personalized care for patients, hence providing a high standard of living, promoting individual patients regiment treatment that is data driven and also according to the physiological conditions optimizing the healthcare devices (Ashton, K., 2009). Figure.2 specifies importance of IOMT in medial industry.

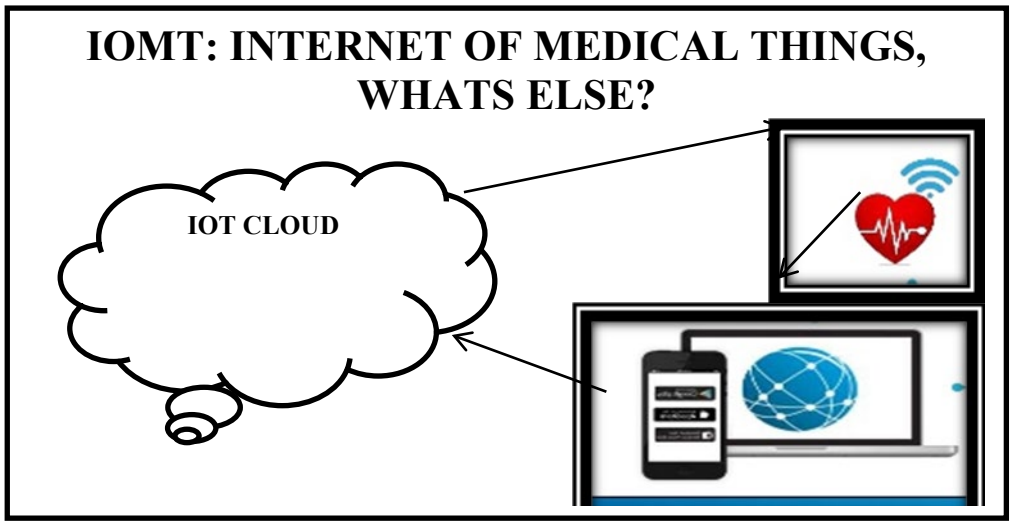


Figure 2. IOMT the Need of Hour in Medical Industry

IOMT provides an ecosystem of connected health through affordable sensors, cloud networks and mobile big data domains. With increase in utilization of IOMT devices and services, leads to increased healthcare frauds which are treated as a white collar crime in present day world. It involves various filings of dishonest claims of healthcare, DOS and malware attacks on user sensitive data stored in healthcare database for profit turning or illegitimately accessing healthcare services. The healthcare frauds and attacks lead to intentional deception or misrepresentation of an individual's entity causing unauthorized benefits to an individual or an organization (Baker, L. A., 2014). Figure.3 depicts various parameters of attacks and frauds on IOMT devices and data.

Figure 3. Parameters of Medical Breaches
http://www.iritech.com/blog/biometric-healthcare/

There are various forms of fraudulent health care schemes that include false statement, deliberate omission or misrepresentation by a healthcare recipient for gaining payable benefits. The attacks and frauds of IOMT are criminal in nature varying from state to state and country to country leading to deployment of "biometrics" as a security solution for this sector. Biometrics is defined as the measurable physical and behavioural characteristics of an individual for establishment and verification of its identity (J.Daugman 2004; Blair, L. M., 2016).The biometrics pattern includes:

- Fingerprint
- Iris Scan
- Palm Prints
- Gait
- Facial Recognition
- Voice Recognition

Figure.4 represents various biometric traits that are utilized for verification and authentication.

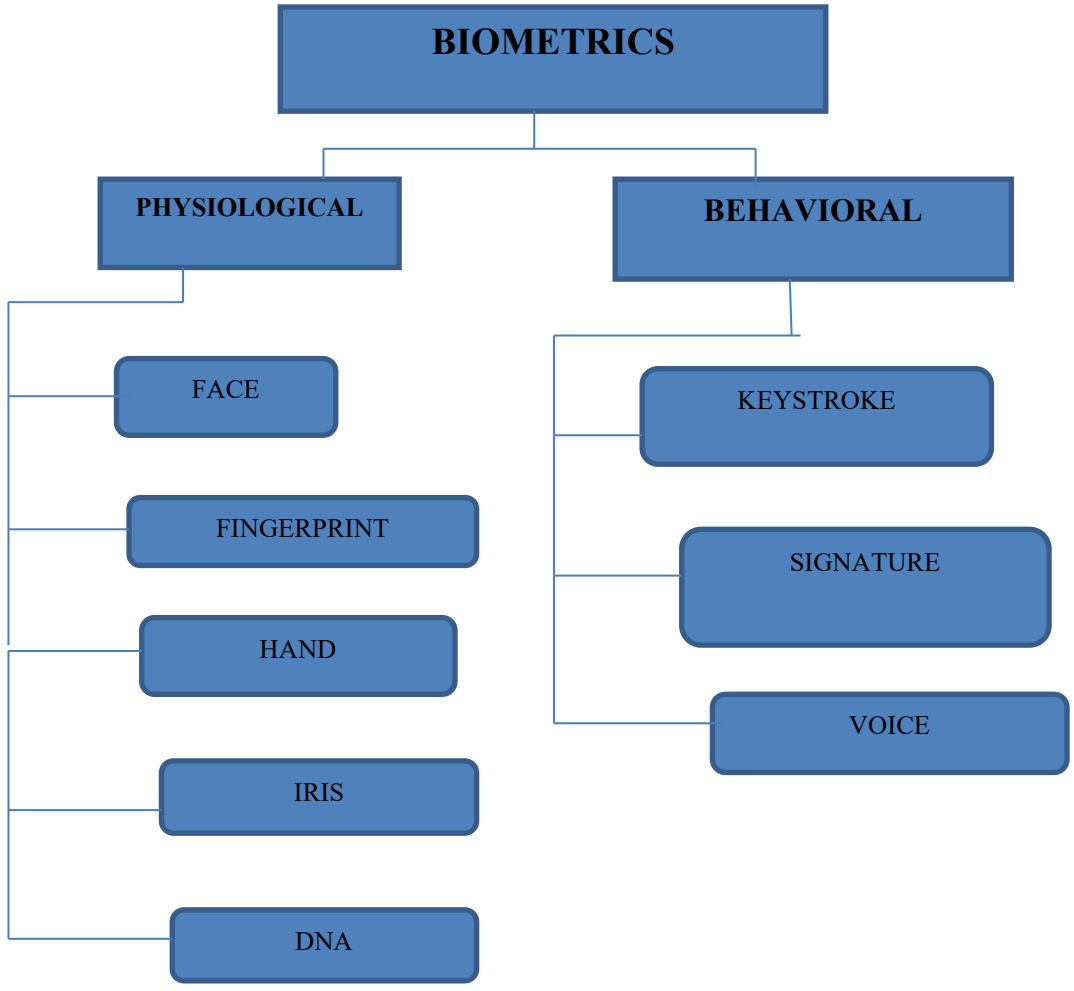


Figure 4. Biometrics Traits Utilized for Verification and Assessment

Biometrics science recognizes an individual based on his/her physical as well as behavioural traits. The Biometric Based Internet of Medical Things (BBIOMT) Authentication Systems are much more reliable than the traditional password systems for individual verification and ensuring their identities.

2. Internet of Things (IOT)

Today in the digital era, analysts evaluate that by year 2020 IOT development of remote associated gadgets will surpass the value of forty billion. IOT is an arrangement of computing integrated gadgets, mechanical and computerized machines and items, various creatures and individuals. Various IOT devices, gadgets, machines, individuals, creatures are all furnished with an identifier that exchanges information along the system with no PC (Personal Computer) and human intervention. Figure.5 represents rise in Internet usage from year 2012 onwards that leads to development of IOT. IOT is gaining attention both at workplace and outside for impacting life and work. Use of IOT leads to reduced loss, costs, wastes and repairs, reviews and supplants items having new or past expiry dates. A basic example of IOT is a smart fridge causing alerts about no milk through the internal camera inside. This research study presents internet as an essential part of day-to-day life, future web-vision and security issues and other gigantic difficulties for IOT world (Brewka, G., 1996).

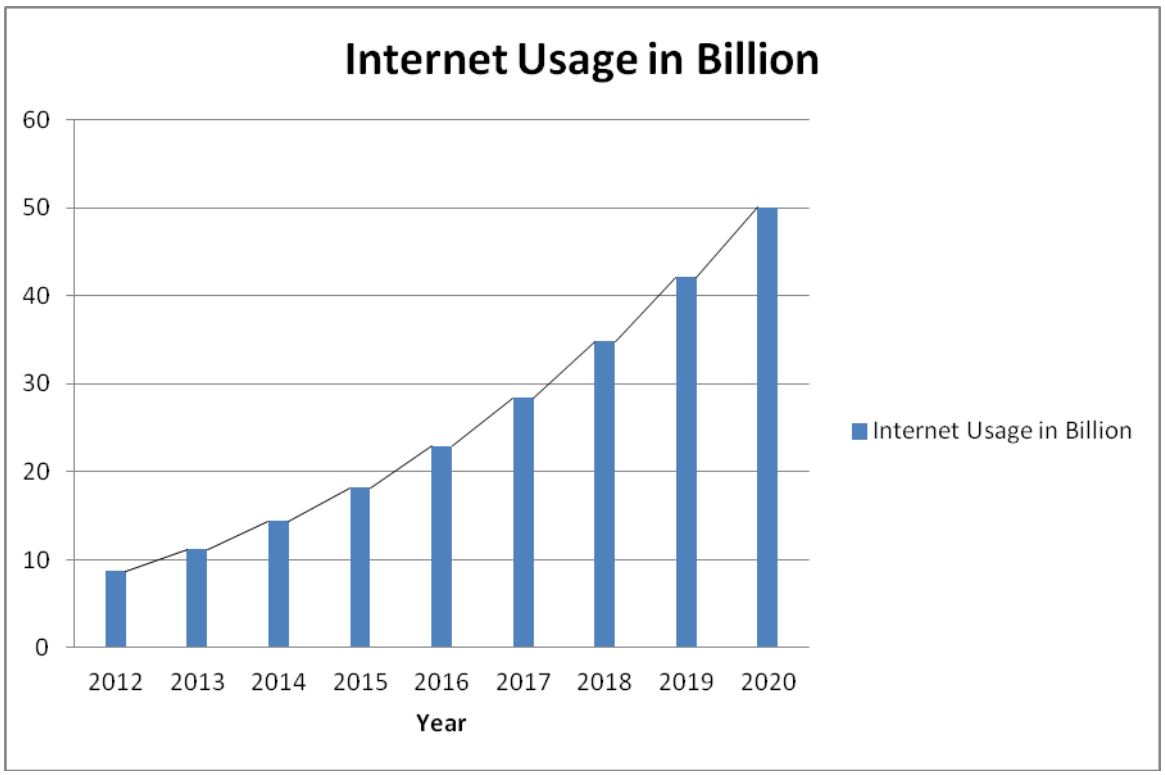


Figure 5. Rise in Internet Usage from Year

3. IOMT

Relating IOT to broad terms it's a collection of various interconnected devices and applications that are interconnected devices and applications that are linked through online network of computers. Its subdivision IOMT (Internet of Medical things) deals with the interconnection of medical devices and equipment that are related to Medicare-IT and Healthcare-IT. IOMT devices are equipped with a wi-fi or some near field communication (NFC) technology that allows machine-to-machine (M-M) communication. 30.3% of IOT devices are utilized in healthcare. IOT economic impact is expected to rise from $3 trillion-$6 trillion in 2025, connecting about 31 billion devices and 4 billion people together. IOT in healthcare is predicted to raise around $2.5 trillion by year 2025. Healthcare stands 3rd most utilized sector for IOT where around 60% of healthcare organizations are utilizing the Internet of Things technology and around 87% organizations are planning to implement the services of IOMT in their usage by 2019 making IOMT the most utilized technology

in the upcoming years (Cercone, F'IEEE, N., Chan, H. C. Y., 2015).

3.1 IOMT Categories

Despite various issues exist, but IOMT has increased the medical industries workforce productivity and reduced the costs of medicare to large levels. IOMT solutions generally fall into the below mentioned categories:

1. Clinical Efficiency: Delivery of medicare devices is improved by utilizing IOMT by various hospitals and dedicated clinics. IOMT devices are utilized for tracking visits of patients from even the most remote locations. Patients and medical equipment location tracking is done by IOT sensors. Tracking of medical adherence is developed by IOT utilized pill bottles.
2. Consumer/Home Monitoring: Self-monitoring for consumers and collection of biometric information is done by IOT technology. For e.g. smart thermometer that reads the temperature utilizing temperature sensors present in smartphones and other devices, ECG (electrocardiogram) done at home are all applications of IOT. IOMT devices help in tracking and collection of patient information from home and also provide assistance in the services of telemedicine.
3. Fitness Wearable: IOMT based biometric sensors are utilized in settings of clinics and hospitals. Heart patches, armlets monitoring blood pressure are connected to the clinical monitoring devices (CMD) that are located at various distant places. "Auto refractor" based smartphones applications utilizing IOMT for vision testing are popularly utilized nowadays.
4. Brain Sensors/Neuro-technology: Cranial wearable are in progress developed by researchers targeting high-tech consumers. IOMT devices are well capable for brainwaves reading, tracking and transmitting patient's mental health. Drug efficiency analysis is being performed through researches on non-evasive neuro-tech (brain wave reading/recording).
5. Infant Monitoring: IOMT enabled wearables for monitoring and tracking infant moments, temperature and pattern of sleep to the parents is another application of IOT. It provides assistance for parents as they are aware of their baby's physical health condition and then respond accordingly.
6. Sleep Monitors: Tracking and monitoring of sleep is utilized for treatment of various neuropsychological disorders; as another application of IOMT. These IOMT monitoring devices continuously send reports to various clinics at distant locations. IOMT applications that are smart-phone enabled are connected to various sleep monitors for further regulating patterns of sleep without clinical intervention. Figure.6 depicts various IOMT categories and their utilization in modern day world

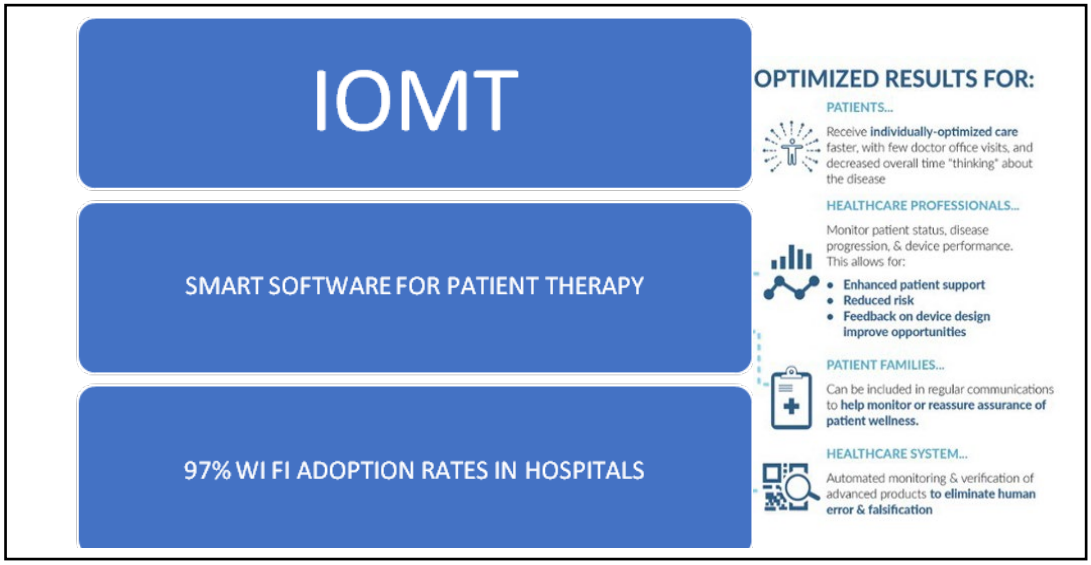


Figure 6. IOMT Utilization in Modern World

3.2 Advantages of IOMT

IOMT in today's world provides a large number of advantages related accompanied with various concerns and future requirements that are listed below:

1. Improvement in the outcomes of treatment as patient care monitoring and deliverance is done round the clock.
2. Costs of medicare facilities are decreased due to real time as well as remote monitoring of patients which leads to fewer clinical visits.
3. Disease management has shown visible improvement as careful real time monitoring is being provided to patients.
4. Patient experience is enhanced as they get complete as well as customized treatment and care.
5. Drug management is also improved due to IOT growth as the IOMT devices and applications assist in research of drug, their deliverance as well as adherence (Kranz, M., 2016).

3.3 Concerns and Future Requirement of IOMT

The concerns and future requirements of IOMT are briefly discussed below:

1. Sensor technologies based innovations are driving IOMT platform as these intelligent networks will be the major future of internet world.
2. IOMT growth will be assisted by development of high speed cloud based computing platform.
3. Large amount of big data is processed through advanced analytics performed through IOMT devices.
4. Round the clock IOMT based patients data should be secured from various attacks. Figure.7 shows the various levels through which IOMT data travels.

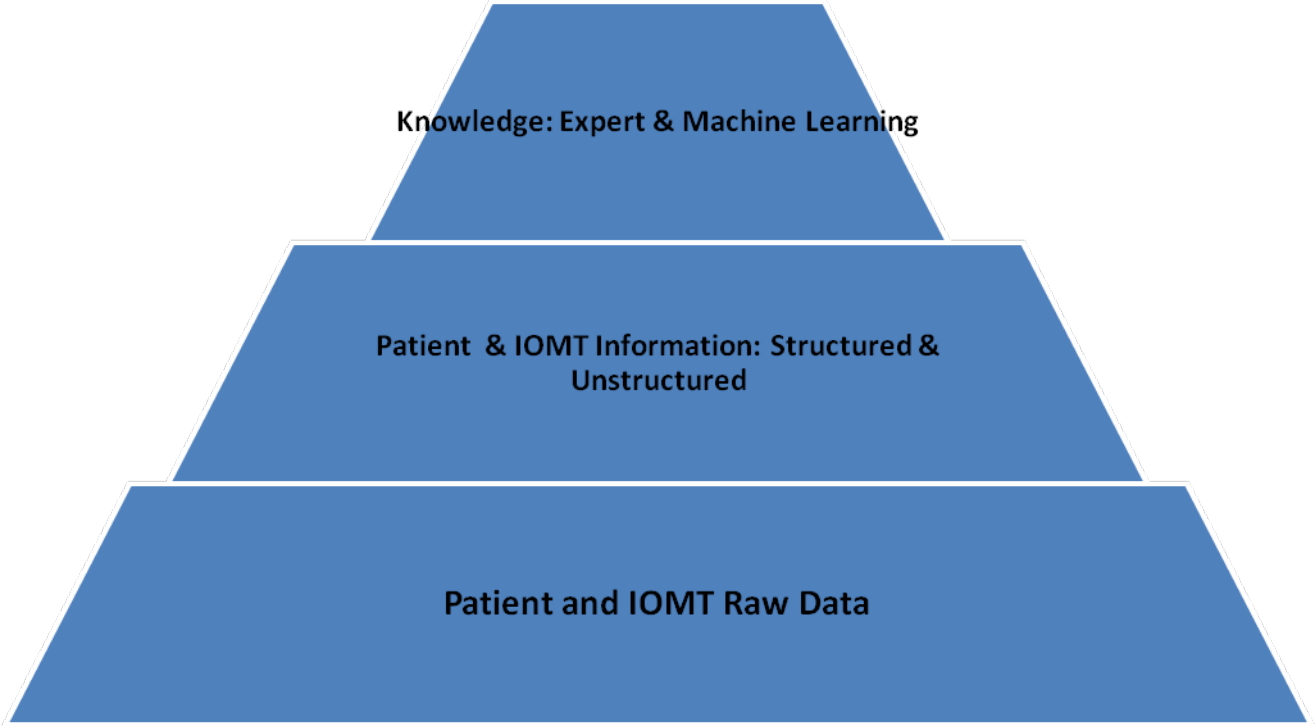


Figure 7. Levels of IOMT Data

3.4 Real World Applications of IOMT

Traditional and existing medical devices are upgraded to modern IOMT devices for real-time sensing of data for monitoring the patients by various enhancements of IOMT devices like sensors, signal converters and communication based modems that can perform remote communication:

- Wearable Devices
- Home-use medical Devices
- Point-of care kits

IOMT devices are utilized in various situations of emergency like:

- Disease Prevention
- Fitness Promotion
- Remote Intervention

Table.1 discusses the key applications and Utilization of IOMT.

Table 1. discusses the key applications and Utilization of IOMT.

S.no	Application	IOMT Utilization
1.	**Management of Chronic Disease**	Devices that are IOMT enabled are providing alternative for management of chronic diseases like: • Hypertension • Cardiac failure • Diabetes The IOMT enabled devices monitor body parameters like • Random blood sugar levels • Weight and electrolyte concentrations inside the body Vital data that is real time is sourced by the IOMT devices which are utilized for future treatment alterations, changes of dose and prediction of progress of diseases. The research studies on epidemiological trends of various diseases for a specific population is furthermore changed and enhanced through IOMT enabled data collection (Chesbrough, H.2010).
2	**Living Assisted through Remote Monitoring (Tele Health)**	The physician office is utilized as a central registration location of data from various network devices. Patient specific data is compiled, processed for healthcare automation and analysis of fresh data is performed against various past records which decide upon the management of patient against future courses. Thus tasks of data routing, it's monitoring and proper field administration is intelligently machine enabled through IOMT machines saving costs of implementation of follow-ups and infrastructure utilization. Remote monitoring has also led to decrease in the rate of member drop-outs and increase in productivity of healthcare resources. Cardiac monitoring is performed through commercialized Body Guardian Remote Monitoring System (BGRMS) that maintains data security as it separates identification information of patients from its observation (Davenport, T. H., & Lucker, J. 2015).
3	**Preventive Care Wellness and Assessment of Lifestyle**	Health supervision through diet, various physical activities and life quality is digitized through IOMT enabled innovative devices like: • Wearable devices • Implantable chips • Embedded systems • Advanced sensors The innovative devices keep track of patient's vital data changes and events of various health conditions at local level and expert assistance during situations of emergency at various locations of remote access.
4	**Remote Intervention**	During emergency real time data that is obtained through sensors helps the physicians for drug administration. The timely reports help in high-tech medical assistance which reduces hospitalization costs (Dhar, V. 2014).
5	**Improvement in Drug Management**	Radio Frequency Identification (RFID) tags that are IOMT enabled help in the management of problems related to drug availability and their related costs of supply. IOMT enabled medication solutions like WuXi Pharmatech and TrugTag have led to the development of IOT enabled edible smart pills that monitor patient's drug doses and pharmacodynamics. These solutions help the drug companies is mitigating risks as well as losses during the administration of supply chains (Deloitte, 2017).
6	**Other Applications**	• Paramedical staffs training courses and coaching. • Rehabilitation and hospitalization assistance. • Health information access to health records without losing medical information. • Online analysis of protein and composition accuracy. Figure.8 represents the IOMT applications utilized in modern world

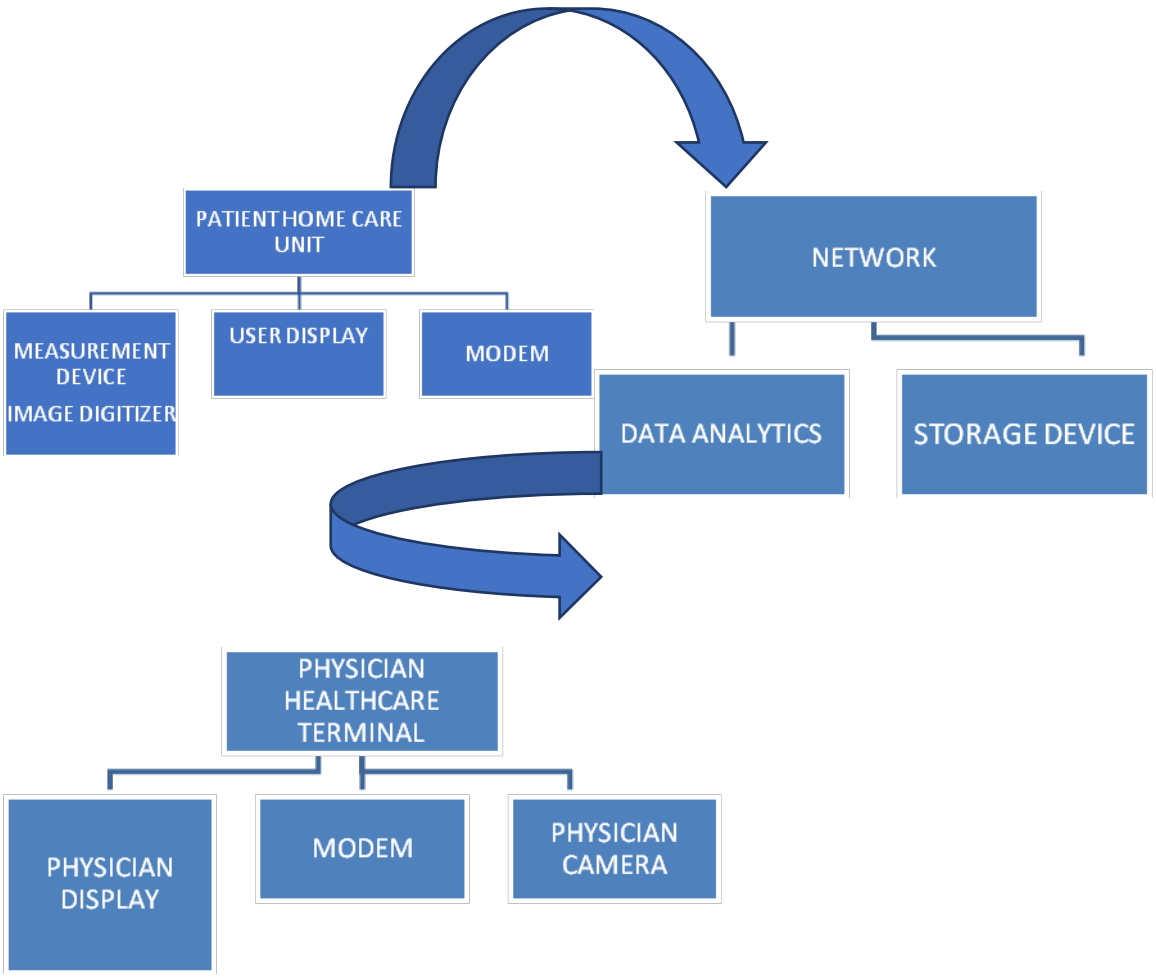


Figure 8. Application of IOMT

3.5 Cyber Attacks in IoT

73% of organizations of medicare are utilizing IOT for monitoring patients and other research studies hence posing lot of concerns of data security. Recently around 89% of healthcare utilizing IOT has suffered from various security breaches. IOMT interconnection of various devices causes personal information as well as business data to be passed on to the cloud and forth along thousands of devices that leads to various exploitable vulnerabilities. One of the serious concerns is privacy in all the devices, applications and systems that share information. Users take precautions to secure data but many-a-times conditions goes beyond their control (Geng, H., 2017). Attacks of unprecedented sophistication are crafted by hackers that not just only correlate information from various private sources like:

- Cars
- Smart phones
- Home
- Automation systems
- Refrigerator etc.

Following are the various attacks that commonly occur on various IOMT devices:

1) Denial of Service (DOS)
DOS attack lead to inaccessible services due to overburdening limits and other parameters. DOS causes malicious attacks in distributed system by causing botnets. Distributed Denial of Service (DDOS) is a subversion of DOS attack. Botnets are the multiple connected services that are online which are involved during a DDOS attack to overwhelm a targeting website by sending fake traffic. Breaching of security parameter is not done during DDOS assaults, rather than website and server services are made unavailable for legitimate

users (Ma, D. (2007). The main features of DDOS attacks include:

a) Its highly noticeable event that impacts the entire base of user online.
b) It's a popular weapon for various;
   - Hacktivists
   - Cyber-vandals
   - Extortionists
   - Champions of web that want to prove their point to world.
c) These attacks last for days, weeks, months and at various times are extremely destructive for various online organizations.
d) They causes losses to revenue, erode the trust of customer, businesses are forced to spend fortunes for compensations and cause damage of reputation for long terms
e) Unlike regular attacks where perpetrator utilizes a single connection of Internet for exploiting software vulnerability, flooding of fake requests for target is an attempt for exhausting the resources of server like CPU and RAM; the DDOS attacks are launched through various connected devices which are distributed all across the Internet.
f) The DDOS are multi-person and device barrages that are quite harder to deflect due to enormous amounts of involved devices.
g) DDOS attacks are targeting towards networks infrastructure for saturating traffic volumes unlike the single source DOS assaults counterparts.
h) Their execution is also different from normal attacks as DOS are launched through homebrewed scripts or the DOS tool like: Loworbi ION Canon; the DDOS assaults are launched through botnets which are large clusters of various connected devices like: cellphones, router etc. which are infected and allow attackers remote access.

Categories of DOS attacks include:

- Attacks at layer 7 i.e. Application Layer Attacks: These are DOS or DDOS threats that overload a server by sending huge number of requests for processing and resource-intensive handling. The application layer attacks include:
  a) HTTP floods
  b) Slow attacks e.g., Slowloris or RUDY
  c) DNS query
  d) Flood assaults

  The application layer assault size is measured typically in request per second (RPS). Around 50-100 RPS is required for crippling most of the websites that are mid-sized.

- Attacks at layer 3 and 4 i.e. Network Layer Attacks: The network layer assaults are DDOS assaults that clog the "pipelines" which connect the network. The network layer attacks include:
  a) UDP flood
  b) SYN flood
  c) NTP amplifications
  d) DNS amplifications

They prevent the servers' access, causes severe types of operational damages like: suspension of accounts and huge overage charges. These assaults are like high-traffic events measured in giga-bits /sec(gbps) or packets/sec(pps). The network layer assaults exceed to around 200gbps but 20-40gbps tend to completely shut the network infrastructures down.

Motivations of Attacker for DDOS:

The attacks are mostly launched by various individuals, businesses and nation–status motivations that include:

a) Hacktivists: The hacktivists DOS assaults are utilised as means of achieving criticism for governments, politicians and and current business events. They follow the principle that "If we disagree, your site goes down" i.e. "Tango Down". The hacktivists are lesser technically savvy and use premade tools for waging assaults on their targets. "anonymous" group is the popular most hacktivist group which in February 2015 cyber attacked ISIS in Paris office and in June 2014 against the Brazilian world cup sponsors (Gong, A., 2013).
b) Cyber-vandalism: "script kiddies" is a referral name for cyber vandals as they rely on premade scripts and tools for causing grief on the fellow citizens of Internet. They are bored teenagers that look for rush for adrenaline, or vent anger, frustration against a school or

institution or against a person that has wronged them. Some cyber vandals are just teenagers seeking attention and respect of their peers. They use DDOS for hiring services of booters and stress for little as $19 a pop (He, D., & Zeadally, S 2015).

c) Extortion: They are the cyber-attacks criminal type activities that demand money in exchange for stopping i.e. not carrying out crippled type of DDOS attack. The companies that are at the receiving end of the DDOS notes that goes offline to succumb after refusing extortionist threats are:
   a) Meetup
   b) Bitly
   c) Vimeo

d) Basecamp

Like their counterpart, cyber-vandalism is enabled by the stresser existence and booter services.

- Personal Rivalry: These attacks are utilized for settling personal scores or disrupt their online competitions. They mostly occur as multiplayer online games, which are launched DDOS barrages against each other, against gaming servers to edge gain or for avoiding imminent defeat by causing the "flipping the table" condition. The attacks on the players are DOS attacks that are executed on the widely available malicious software attacks on servers that are launched from the booters and stressers (Mahoney, B. 2012).
- Business Competition (BC): The BCDDOS attacks are increasingly utilized as competitive tool of business, designed to drag away a competitor in participating for a significant event like "Cyber-Monday". Some BC assaults are launched to completely shut-down the online based business for months and years. They cause disruption that well-encourage financial damage of customers and affect business reputation. The business feud BC attacks are quite funded well and executed through professional "hired guns" that have conducted scary reconnaissance and utilize proprietary wots as well as resources for sustaining the heavily aggressive DDOS assaults.
- Cyber-Warfare: They are the state sponsored DDOS assaults that have the aim to silence the global critics and internal opposition. They work as a means for disrupting critical services of finance, health and infrastructure of the enemy countries. The cyber-warfare attacks are backed by nation, states and are well funded.

Preventing DDOS attacks:

The DDOS attacks are difficult to prevent as the cyber criminals attack their targets regardless of their defences. The brewing storm of DDOS can be spotted by the following:

i. Monitoring traffic against abnormalities like: traffic spikes that are unexplained, suspected IP address visits and geo-locations. They could be "dry-runs" from attackers for testing the defences before the full-fledged attack. Recognition of the abnormalities can help preparing the onslaught.
ii. Keeping eye on social media like Twitter, public waste-bin like: Pastebin.com against threats, boats and the conversations that hit the incoming attack.
iii. Consideration of the third party DDOS based pen-testing for simulating attack against IT infrastructure to prepare against moment of truth.
iv. Creation of a response plan and a rapid response tea for minimizing the impact of assault. They include customer support based communication teams.
v. It's important to choose a correct mitigation strategy. As rightly said by Richard Clarke of National Security Council (NSC) "If you spend more on coffee than on IT security you will be hacked. What's more you deserve to be hacked". For preparing against DDOS incidents leads accessing the risk that includes answers to the following questions:
   - Which level of assets of infrastructure requires protection?
   - What are the soft spots (SS) or the single failure points?
   - What's required for their shut-down?

- How and when you are targeted and when it will be too late?
- What are the financial impacts against an extended outage?

vi. It's important to prioritize concerns after examination of various DDOS based mitigation options within the security budget framework. A commercial website or online SAAS banking e-commerce protection, a law firm wants protection of its email, FTP servers, back office platforms, business require "on-demand" solution.

vii. It's important to choose the deployment method. The Border gateway routing protocol (BGP) is the most common and effective way for deployment of the core infrastructure services across the subnet. It works on-demand on manual activation of the security solution.

viii. A DNS redirection for re-routing all the HTTP and HTTPS traffic is an always-on DDOS protection for the web application. They absorb volumetric assaults, minimize latency and accelerate the content delivery.

ix. Network layer attacks require additional scalability through BGP announcement for ensuring routing the incoming traffic to a set of scrubbing centres. It has the capacity to process hundreds gbps of traffic. Scrubbing centres have powerful servers that filter out the malicious packets forwarding only the clean traffic through the tunnel. It provides protection against the direct-to-IP attacks being compatible with all infrastructures and communication protocols like: UDP, SMTP, FTP, VOIP etc. Figure.9 shows the amplification attack scenario.

x. Traffic profiling solutions are utilized for application layer attacks mitigation to distinguish between malicious bots and website visitors who are legitimate signature and behaviour based heuristics, IP reputation scoring, cookie challenges are best practices for traffic profiling. The filter out malicious traffic protect against application layer attacks without impacting legitimate visitors. Figure.10 specifies the most affecting cyber-attacks on IOMT devices and services.

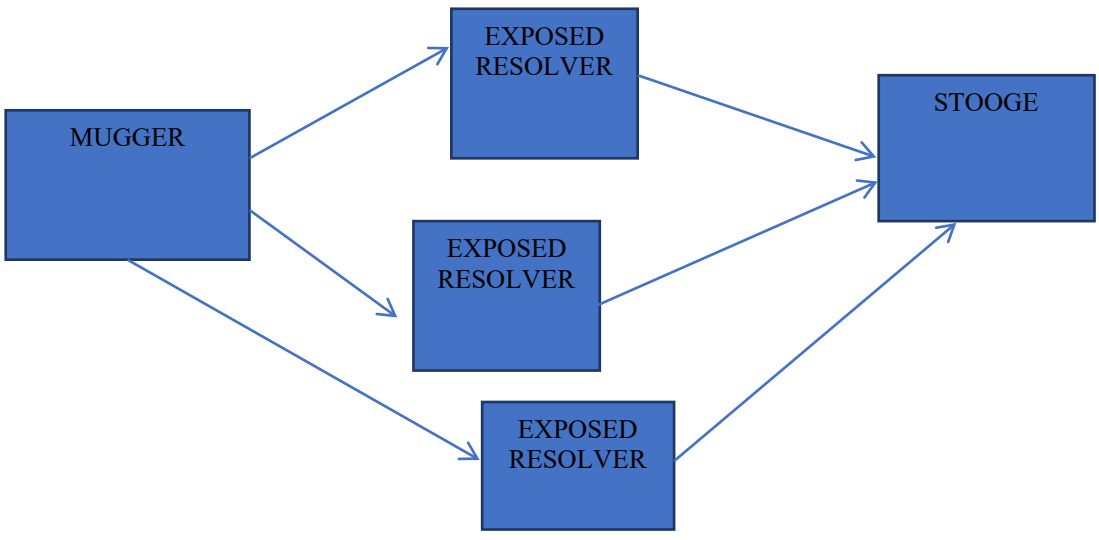


Figure 9. Amplification Attack Scenario

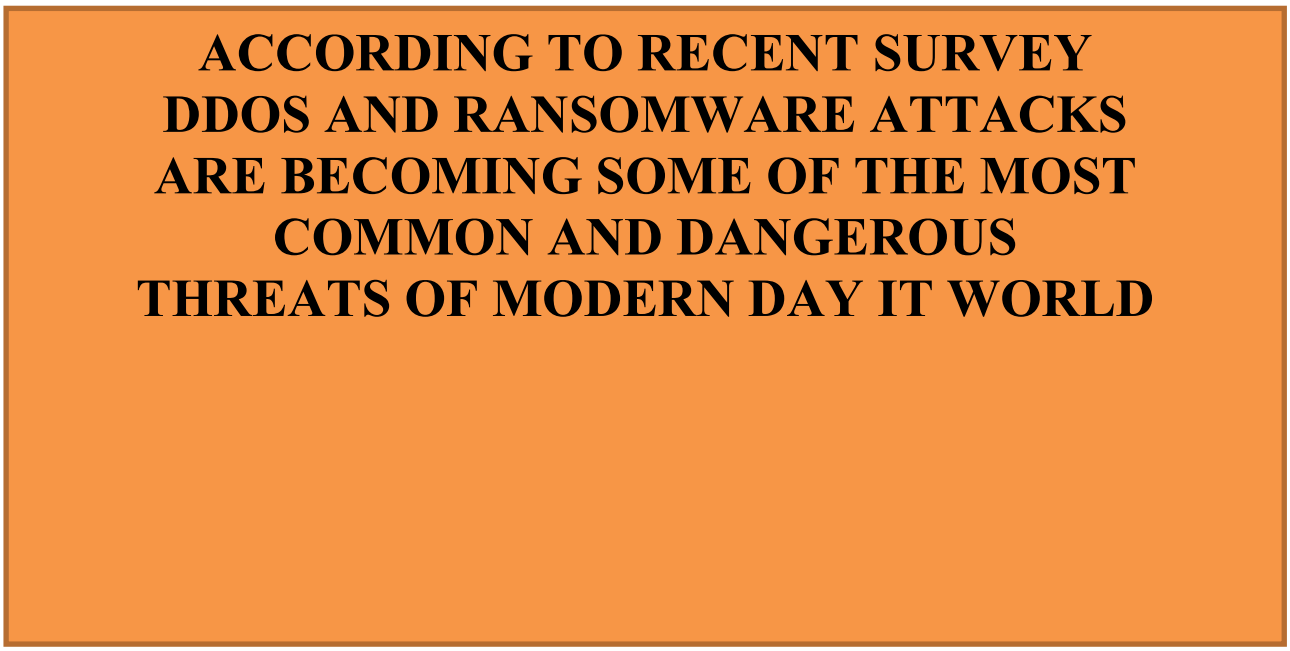


Figure 10. Latest Cyber Attacks in IOT

3.6 Ransomware

Cyber-attacks are rising at a great rate affecting critical services despite of the efforts by security professionals to prevent them. Ransomware attacks are gaining attention as they capitalize on the victims fear factors. Phising emails, direct downloads, scare tactics as utilized by attacker in ransomware attacks to prevent or restrict access of critical data files. A highly profitable business model is evolved through ransomware attacks by criminals as they utilize sophisticated encryption methods, advanced options of payment for extorting money and enticing users to realize its real potential. About 100 new ransomware families in year 2015 were identified as revealed by Symantic a leading global cyber security organization. Ransomware has led to losses of 100's of millions of dollars as the attack is self-propagating and has the potential and power for infecting the entire organization. They restrict the user access as they encrypt most sensitive data files and lock down system completely. They focus on direct generation of revenue as the perpetuators use the scare tactics for demanding a huge ransom for service restoration. Bitcoins is the most preferred method of payment utilized by ransomware attackers. Bitcoin is a digital currency that has non traceability during online transactions of money. Crypto-ransomware is the most common type of ransomware attack that aims for encrypting sensitive data files of victim. Locker ransomware locks the victim's computer and devices access is the second most common type of ransomware attack (Mell, P., & Grance, T., 2011). Figure.11 focuses on the percentage of ransomware attacks on different IOT based services.

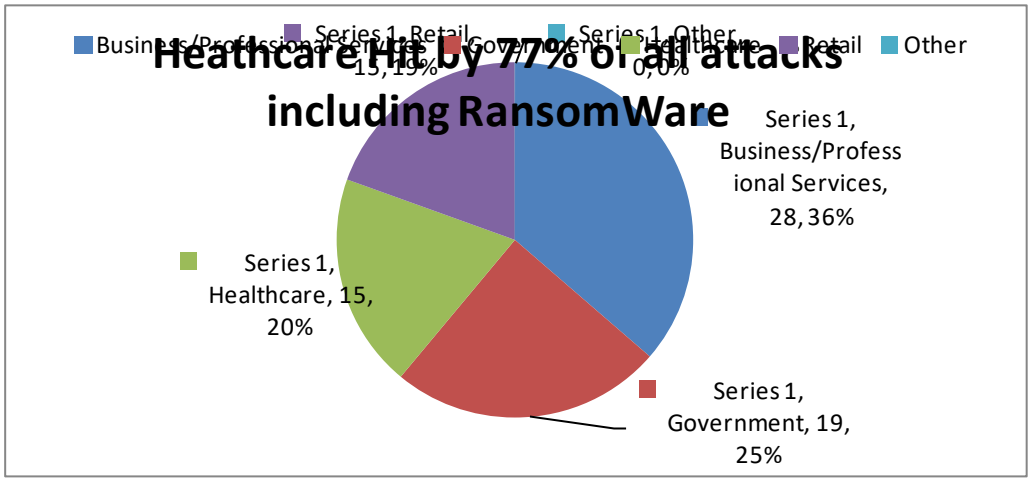


Figure 11. Percentage of Ransomware Attacks on Different IOT Based Services

Target and Ransomware Attacks Implications:

The objective of ransomware assaults can be the customers and associations which incorporate home clients, little to huge organizations, open or Government offices, and even legislators/famous people. The ransomware assaults target touchy data including business recommendations, individual data, bank points of interest, passwords, client data and so forth which can make disastrous impacts in business or in the life of people. The client won't have the capacity to get to a ransomware hit machine as the assailant takes control of the basic documents and encodes it. The results of ransomware assaults incorporate loss of delicate data either briefly or for all time, interference in the standard task or working of administrations, money related misfortunes and in addition reputational harm for the people in question. In a large portion of the occurrences, the recuperation of information will be to a great degree troublesome and may require the help of information recuperation authorities (Raghupathi, W., 2010; Ripberger, J. T. 2011).

Working of Ransomware:

There are different techniques in which a ransomware can hit a shopper or an association. One of the conspicuous techniques to spread ransomware is through malignant spam messages, which are generally disseminated utilizing botnets. This can occur through social designing strategies or direct download too. The email or the downloaded document contains a vindictive connection and once the injured individual access this, it can encode the information inside the framework or can bolt the framework dependent on the kind of the malware. The server at that point advises the injured individual requesting a ransomware to decode the records or open the framework. The assailants may initiate the dread strategies by acquainting a commencement clock the payoff, which for the most part says once the due date is crossed it will annihilate the encryption key or twofold the payment sum. Clearly, paying the payoff isn't an assurance as the shopper or association may in any case free the records even after the installment of payment (Ruths, D., & Pfeffer, J., 2014; Schatsky, D., & Trigunait, A. 2011; Schellevis, J. 2014).

Protection against Ransomware Attacks:

1. Consumers, independent companies and undertakings must execute multilayered barrier systems while managing ransomware assaults. Organizations must utilize standard information reinforcement and recuperation anticipates all the basic information they store. The reinforcements ought to be tried and the upheld up information must be put away in independent gadgets ideally dis-connected.
2. Regular patching updates should be performed against the attacks. The application fixes and working framework patches must be cutting-edge and tried to maintain a strategic distance from any potential vulnerabilities. Productive fix administration lessens the odds of assaults through exploitable frail connections.
3. The restricted model of privilege should be followed by the organizations for reducing the installation chances and running of unwanted software applications.
4. The antivirus must be updated and frameworks must be introduced with most recent antivirus

programming and all the downloaded records must be looked over it.

5. Application whitelisting must be implemented by the organizations. Associations must pursue an application whitelisting process which forestalls the framework and system getting tainted with pernicious or unapproved applications.
6. User awareness will be created against ransomware attacks. Clients are the weakest connection in digital security and instructing them through appropriate preparing is vital. Security proficient must know about the most recent patterns in this space and need to instruct the clients in regards to spam messages and phishing assaults.
7. Email should be protected against ransomware attacks. Associations must watch out for their messages. They should square email messages with connections from suspicious sources.
8. Endpoint should be protected against the ransomware attacks: Associations must secure the endpoints by keeping malignant documents from running.
9. Good security practices should be nurtured. Associations must keep up great security propensities and safe practices when perusing the web and should defend the information with suitable controls.
10. An integrated approach against ransomware attack should be followed. By following an incorporated way to deal with digital security, associations can to a great extent address the difficulties with tending to the digital dangers including ransomware assaults. Most joyful personalities Digital Hazard Insurance Stage is such an incorporated stage which enables associations to use on numerous security advances progressed and cutting edge organize, endpoint security, giving further examination and experiences to a coordinated way to deal with danger lifecycle. Digital Hazard Insurance Stage is a cloud-facilitated stage and can be utilized in a membership based model. Digital Hazard Insurance Stage is chance mindful, character mindful, information mindful and condition mind-ful stage giving complete perceivability of the security pose (Schilling, M., 2012).

4. Biostatical Techniques for Maintaining Security Goals

As past sections examines, why it is essential to keep up security of IOMT, utilizations of the IOMT in this day and age and diverse kinds of digital assaults in IOMT, this section will examine biostatical systems for keeping up security and protection of IOMT. Biometric is one of the components which can be utilized as biostatical strategies for keeping up security of IOMT. Biometric is a confirmation system which partners client character check process that includes natural sources of information or examination of some piece of body. It is fundamentally a security procedure that relies upon one kind of a natural person to confirm its character. Biometric information is collected and gathered in the database. On the off chance that both the information coordinates then verification is affirmed. Fundamentally these all instrument are done to give security and protection to the IOMT administrations and gadgets (Sherin Zafar, M.K Soni and M.M.S Beg 2015). Figure.12 speaks to the sorts of biometric groups as solid and feeble biometrics.

BIOMETRICS	UNIVERSALITY	UNIQUENESS	PERMANENCE	COLLECTABILITY	PERFORMANCE	ACCEPTABILITY	CIRCUMVENTION
FACE	H	L	M	H	L	H	L
FINGERPRINT	M	H	H	M	H	M	H
HAND GEOMETRY	M	M	M	H	M	M	M
KEYSTROKE DYNAMICS	L	L	L	M	L	M	M
HAND VEIN	M	M	M	M	M	M	H
IRIS	H	H	H	M	H	L	H
RETINA	H	H	M	L	H	L	H
SIGNATURE	L	L	L	H	L	H	L
VOICE	M	L	L	M	L	H	L
FACIAL THERMOGRAM	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L
H=HIGH , M=MEDIUM, L=LOW							

Figure 12. Various Sorts of Biometric Groups as Solid and Feeble Biometrics

There are various sorts of biometric like unique finger impression, confront, DNA, Iris and so on. Some solid biometric are Iris, DNA, confront, retina. Iris is a robotized procedure of biometric distinguishing proof component which utilizes scientific acknowledgment methods on video pictures of either of the iris of people. The different reasons which made iris acknowledgment framework as one of the most grounded biometric instrument are listed below(Steinbrook, R., 2008; Sweeney, L. 2002):

- Stable – The interesting example in the human iris is shaped by 10 months of age, and stays unaltered all through one's lifetime
- Unique – The likelihood of two ascents delivering a similar code is about unimaginable
- Flexible – Iris acknowledgment innovation effectively incorporates into existing security frameworks or works as an independent
- Reliable – An unmistakable iris design isn't powerless to burglary, misfortune or trade off
- Non-Invasive – In contrast to retinal screening, iris acknowledgment is non-contact and snappy, offering unmatched exactness when contrasted with some other security elective, from separations to the extent 3″ to 10″. Subsequent to performing writing overview, the different customary security systems that are use in IOT and their assaults and disadvantages are recorded beneath in the Table.2.

Table 2. Different Customary Security Systems that are used in IOMT and their Assaults and Disadvantages

S No.	Name of Mechanism	Description of Mechanism	Different attacks or drawbacks
1	Advanced Encryption Standard (AES)	AES is a symmetric square figure, which is favored by the US government to encode the delicate information around the world. It is anything but difficult to actualize on different equipment and programming and in addition in an exceptionally limited condition. Different highlights of AES are secure, cost effective and it is outfitted for managing 128 pieces square while using key estimated at 128, 192 and 256 bits. It uses a substitution change framework and work on 4*4 systems.	AES is powerless against Man-in-middle assaults.
2	High security and lightweight (HIGH)	HIGH is used for basic operation like XOR operation on fiestel network. Key for HIGH is generated while encryption and decryption phase. It has a block size of 64 bits with 128 bit key of 32 rounds. Main features of HIGH are it require less power, few lines of code and it improve the speed of RFID.	HIGH is vulnerable to saturation attacks.
3	Bootstrap Security	Security is the most imperative factor in the success of Internet of medical thing. Secure transmission of data will always be challenge for this growing area. Today, generic bootstrap architecture, technology supports data integrity and authentication in IOMT.	To share the initial key with the smart phone or home gateway QR code are required. These QR code is packed in a package of thing and employee of company can easily see QR code and key. Attacker can perform dictionary attack to get key and plain text. Also long and random key can't be stored in the device.[14]
4	Elliptical Curve Cryptography (ECC)	ECC is a kind of public key encryption strategy which depends on elliptic curve hypothesis and which is utilized for making quicker, smaller and effective cryptographic keys. It uses 164 bit keys to	A HP researcher Nigle Smart discovered a flaw in which some curve are extremely vulnerable.[9]

		provide levels of security rather than 1024bit keys used by other system to achieve it. They give comparable security bring down processing force and battery asset utilization. It is a looping line crossing two axes based on condition made by mathematical gathering.	
6	PRESENT	PRESENT is utilized as ultra-light weight algorithm for security. It requires 4 bit input and output s-boxes, works mainly on substitution layer. It works on 64 bit size block and key of 80 or 128 bit.	PRESENT is vulnerable to. Integral attacks. It is powerful technique to recover secret key.
7	RC5	RC5 is firstly proposed by Rivest for the rotations that are data independent. It is used mainly in wireless scenario and work well as a light weight algorithm. It possesses Fiestel structure and works on 32 bit size which can also vary to 16,32,64.	RC5 is vulnerable to differential attacks.
8	RSA	RSA was invented by Ron Rivest, Adi Shamir and Leonard Adleman in 1978. It works by selecting two large prime numbers and then generating public and private key pair of by them. In the wake of finding their modulus and picking encryption key aimlessly and after that figuring the decryption key. In general public key is distributed to everybody and private key is made secure.	It is vulnerable to various attacks like cycle attacks, searching message space, guessing and and so on.

The social insurance framework, during the time spent change to upgrade protected, quality and cost contained consideration, is confronting numerous difficulties. The most major issues that human services framework is encountering are medicinal wholesale fraud, different sorts of misrepresentation in social insurance administrations and social insurance protections. As indicated by Financial Cost of Healthcare Fraud report 2014, the current worldwide normal misfortune rate expanded from 5.99% in 2007 to 6.99% in 2011 equivalent to $487 billion. The ongoing report from FBI expressed that "Medicinal services extortion costs the nation several billions of dollars a year. It's a rising danger, with national medicinal services uses assessed to surpass $3 trillion out of 2014 and spending proceeding to outpace swelling**".** (Viju Raghupathi, W. R., 2013; Walker, R., 2015).

The best answer for avoid misrepresentation and restorative data fraud in human services is to reinforce the confirmation and limit the dangers of security ruptures with the utilization of biometrics. Biometrics has been turning into the best decision for the medicinal services supplier to fathom fake issues. As of late, biometrics has being embraced by different human services associations worldwide to secure wellbeing records, encourage simpler access to medicinal data, and guard social insurance shoppers against cheats. Moreover, the ascent of interoperable wellbeing data databases utilizing biometrics can empower administrations to just and consistently administrate the entrance to medicinal personality by approving access to patient's records utilizing biometric character. By connecting such data, the patients can be effortlessly distinguished and associated with their own restorative records accommodating particular medicinal services administrations. Consequently, the connecting among biometrics and electronic wellbeing records enables the wellbeing associations to give more precise and effective social insurance administrations. Since April 2009, the US requires the doctors and human services experts who utilized electronic wellbeing record should check painstakingly the getting to the patient's record. Biometrics enables the doctors to do this effectively. By making the records just open to somebody who is distinguished by unique mark, vein or iris, a record can be kept of personality and time getting to the document, and it very well may be guaranteed that the individual who got to the document is certainly the one has the privilege to see a patient's record. On the off chance that they jumble, the fitting specialists can be told that unapproved individual is endeavoring to get to anchor information (White, S., 2014).

Human services biometric advertise has imagined a gigantic development in the previous couple of years. As per “Medicinal services biometrics advertise” report from

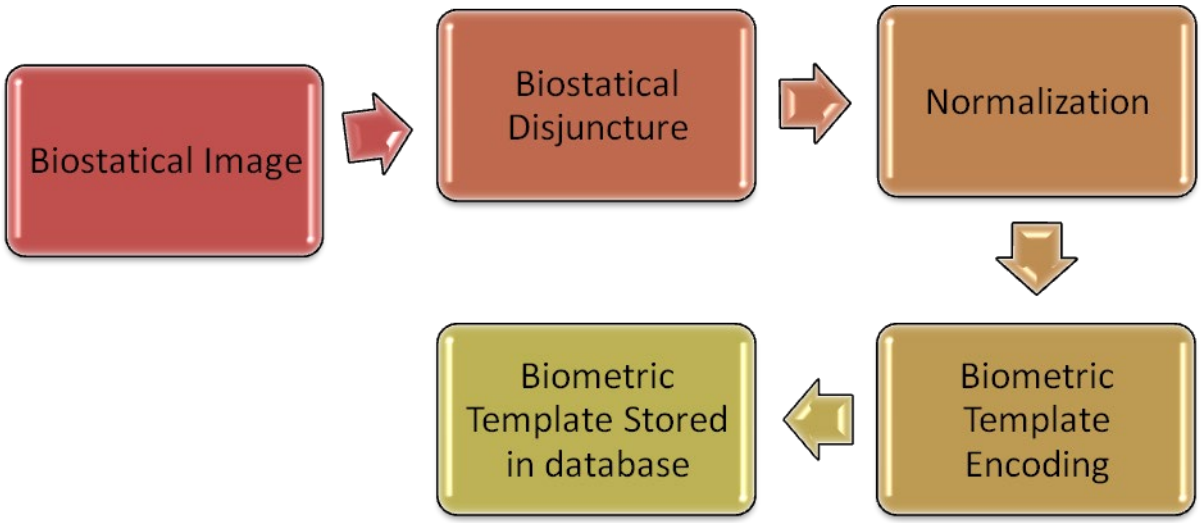
Transparent Market Research distributed on September 2013, the unique finger impression acknowledgment innovation is the most unmistakably utilized biometric innovation and will make up over half percent of biometrics request in human services industry through 2019. Additionally, face and iris acknowledgment are likewise anticipated that would have quick development in term of the interest for consistent access control in social insurance administrations. As of now, North America alongside Europe catches over 75% of the piece of the overall industry. The worldwide social insurance biometrics showcases cost of $1.2 billion out of 2012 is anticipated to ascend by 25.9% from 2013 to 2019 with the evaluated market estimation of $5.8 billion of every 2019. Human services has turned out to be one the most alluring markets that numerous biometrics organizations plan to infiltrate in including 3M Cogent, Inc., Bio-Key International Inc., DigitalPersona Inc., NEC Corporation, M2SYS LLC (Wilkinson, Z., 2013;Yin, R. K., 2013).

There is almost certainly that biometrics has huge potential in human services, in encouraging cost decreases, upgrading data security, expanding the administrations quality, enhancing availability, and much more noteworthy geographic value of conveyance. To push biometric innovation into the standard ID advertise, it is essential to support its assessment in reasonable settings and encourage development of modest and easy to use executions.

5. Consociate Healthcare IT System through Biometric Based Internet of Medical Things (BBIOMT) Approach

This research chapter takes note of that "human services biometrics" used for access control, distinguishing proof, workforce administration or patient record stockpiling. Biometrics in medicinal services often takes two structures: giving access control to assets and patient recognizable proof arrangements. The developing interest for biometrics arrangements is essentially determined by the need to battle misrepresentation, alongside the basic to enhance tolerant protection alongside social insurance security. Biometrics is additionally being utilized for medicinal observing and versatile social insurance. The biometric enlistment process starts with endorsers visiting a registration office and giving their biographic data and unique mark tests. Before part information is for all time added to the part database, Automated Biometric Identification System (ABIS) contrasts the unique biometric impression tests and all people as of now in the database. Any copies identified by the ABIS are physically arbitrated by a mediation officer who, bolstered by a devoted programming application, examines every potential copy and chooses which of them to acknowledge as authentic. When this procedure is finished, the framework recovers the significant biometric and biographic data from the local database and in a split second customizes and prints a shrewd card for the par (Yasseri, T., Sumi, R., & Kertész, J.,2012). The whole procedure of catching a part's information, de-duplication, card personalization and printing is commonly finished inside 7 minutes. To check the increasing expense of cases and therapeutic case extortion, biometric confirmation is performed at the social insurance supplier's end. At the point when a card holding part visits a medicinal services supplier, their unique mark information is caught and coordinated against the finger impression format put away on their part card amid enrolment. On the off chance that confirmation is effective, an irreversible case check code (CVC) is produced and entered on the part's case frame. The CVC depends on biographic information, setting data, (for example, medicinal services supplier ID, benefit date and enrolment ID) and the consequence of the biometric confirmation. Since the CVC must be created accurately if the part is available at the time the case is produced, it goes about as a biometric evidence of-nearness, in this way dispensing with phony and copy claims from human services suppliers.

An across the country rollout of the biometric participation enlistment and moment issuance of the ID card framework began in January 2014. Up until this point, more than 4 million supporters have been effectively enlisted utilizing the new framework. The activity to receive biometric innovation in the medicinal services framework is relied upon to prompt a copy free part database, insurance of information uprightness and enhanced effectiveness in administration conveyance. Moment issuance of part ID cards at the purpose of enrolment has likewise dispensed with postponements in ID card creation. These advantages, together with the radical decrease in deceitful cases through biometric validation at the purpose of administration conveyance offer long haul advantages to country's social insurance. As far as appropriation, the interest of biometric human services for patient distinguishing proof arrangements clearly lies with its natural advantages. Biometric ID arrangements offer the choice to distinguish appropriate protection status, in this manner expanding extortion assurance. Another key advantage is wellbeing. With the utilization biometrics, a confirmed patient acquires the right treatment. Figure.13 depicts the Biometric Based Internet of Medical Things (BBIOMT) approach to make the IOMT system more secure against various attacks.


Biostatical Image
Biostatical Disjuncture
Normalization
Biometric Template Encoding
Biometric Template Stored in database

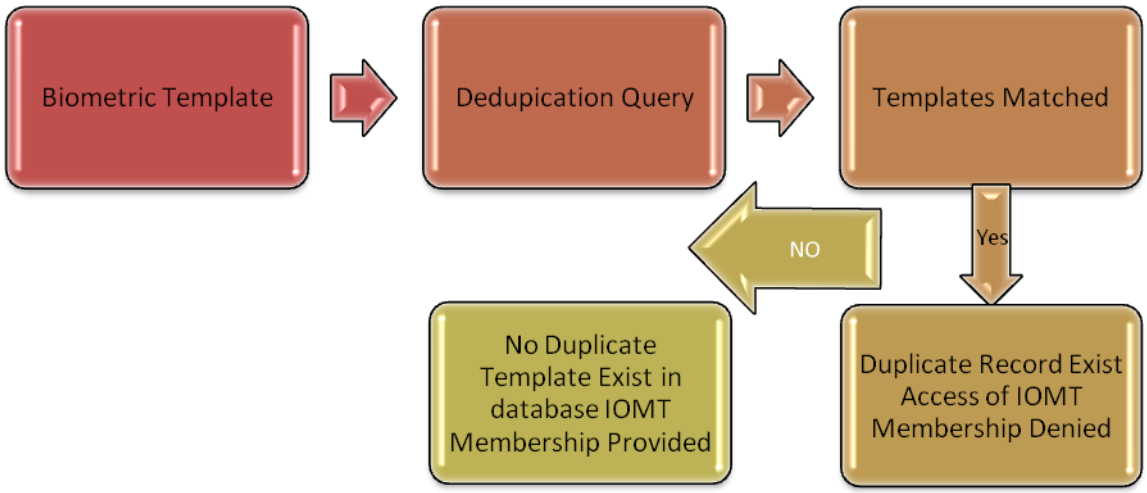


Figure 13. Biometric Based Internet of Medical Things (BBIOMT) Approach

Further, the utilization of biometrics is fast and proficient, disposing of the requirement for entering in information which can prompt temperamental information. These frameworks are likewise advantageous since they work for lethargic patients. The driving goal behind biometric medicinal services is in this way to join high security with accommodation. As associations receive innovative guides that grasp higher security through biometrics, the following obstacle will execute understanding distinguishing proof arrangements and making open systems for patients to get to their medicinal records over a large number of suppliers and stages. With the coming changes to the patients wellbeing framework and as therapeutic record administration capacities change with innovation, tolerant recognizable proof components will without a doubt stick to this same pattern. The abilities and adaptability of biometrics as to tolerant distinguishing proof evacuates numerous dangers of fabrication, misidentification and record security.

6. Conclusions and Future Scope

Versatile wellbeing, otherwise called IOMT, is a term utilized for the act of medication and general wellbeing upheld by cell phones. The term is most generally utilized in reference to utilizing versatile specialized gadgets, for example, cell-phone, tablet PCs and individual advanced partners (PDAs), for wellbeing administrations and data. IOMT is a subset of eHealth, which is the utilization of data and correspondence innovation. IOMT applications incorporate the utilization of cell phones in gathering network and clinical wellbeing information; conveyance of social insurance data to experts, scientists, and patients; on-going checking of patient imperative signs; and direct arrangement of consideration by means of versatile telemedicine. IOMT is an undeniably famous thought in light of its ability to build access to human services and wellbeing related data, especially in difficult to-achieve populaces and in creating nations. IOMT applications can enhance the capacity to analyse and track ailments and can give timelier, more significant general wellbeing data. Further, IOMT applications can give extended access to continuous medicinal instruction and preparing for wellbeing labourers. Biometrics Research Group, Inc. expects that biometric innovation will be exceedingly utilized to secure portable wellbeing gadgets, applications and assets. Unique mark acknowledgment innovation will be used the most since it is the essential biometric innovation used in cell phones and various IOMT devices. For sure, unique mark innovation is in the spotlight because of Apple, Samsung and other gadget producers, who have expelled the persona around biometrics by acquainting the innovation with the purchaser. Unique mark acknowledgment is in this manner turning into a comprehensively acknowledged strategy for positive recognizable proof and anticipated that it will be progressively utilized in IOMT applications. Since wastefulness and extortion are abrogating authoritative worries for human services frameworks interest expansion in social insurance security conventions that include biometrics is being adopted. Selection of "medicinal services biometrics" is done in healing centres, facilities and different offices. As far as work process, these apparatuses will secure medicinal services assets and therapeutic information. Concerning patients, biometric frameworks will be utilized for patient distinguishing proof. While little

scale executions are utilized it's expected that huge scale persistent distinguishing proof frameworks will be taken off in rising and creating nations. Medicinal biometrics will keep on forming into a development showcase because of the expanding interest for "wearable" buyer gadgets. The expanding utilization of IOMT applications will likewise drive the use of biometric validation for security purposes.

While IOMT-based restorative innovation applications are still in a beginning phase of advancement, the execution of associated gadgets could altogether enhance human services conveyance. Maybe the best preferred standpoint would be an upgraded operational proficiency through a developing utilization of arranged gadgets. Straightforward information spill out of lower-level physical gadgets to the cloud (and related information examination) could empower continuous reaction from remote areas, maybe sparing lives now like never before previously. Information driven basic leadership is probably going to engage guardians to precisely screen a patient's complete wellbeing status, take pre-emptive preventive measures, and also momentarily react to crisis circumstances. The interconnected frameworks are estimate to decrease the weight of expense on patients, increment quiet consistence, and use the upsides of savvy gadgets that can give quick responsive human services. In spite of the fact that computerization in medicinal services checking would increment operational proficiency, it might present genuine dangers amid usage, for example, information robbery, uncertain information exchanges, and unpredictable system associations. These difficulties, joined with administrative obstacles, are anticipated to drive development in IOMT-based systems administration and information arrangements. There is still extension to enhance gadget and worldwide information gauges over the business, which would empower information taking care of in a reliable manner. Considering the advantages and related difficulties, IOMT appears an encouraging answer for enhance medicinal services checking and treatment results. By giving individual information driven treatment regimens and streamlined gadgets according to physiological prerequisites, this innovation speaks to another period of customized medicinal services and better expectations for everyday comforts the world over. Ongoing exploration and improvements in sensors, systems, distributed storage and registering, and versatility, and enormous information examination have sufficiently advanced to empower the making of reasonable keen restorative gadgets and an associated medicinal services biological community.

References

[1] Anya, O., & Tawfik, H. (2016). Leveraging big data analytics for personalized elderly care. *Applied Computing in Medicine and Health*, 99-124. doi:10.1016/b978-0-12-803468-2.00005-9.

[2] Aly I.Desoky, Hesham A. Ali, Nahal B Abdel-Hamid (2011). Enhancing Iris recognition system performance. *ICCES, International Conference, Cairo, Egypt.* Retrieved from http://ieeexplore.ieee.org/document/5674902/.

[3] Ashton, K. (2009). That "Internet of Things" Thing. *RFiD Journal*, 4986. Retrieved from http://www.rfidjournal.com/articles/view?4986.

[4] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: a survey. *Computer Networks*, *54*(15), 2787–2805.

[5] Baker, L. A. (2014). Do our "big data" in genetic analysis need to get bigger? *Psychophysiology*, *51*(12), 1321-1322. doi:10.1111/psyp.12351.

[6] Bakker, L., Aarts, J., & Redekop, W. (2016). Is big data in healthcare about big hope or big hype? early health technology assessment of big data analytics in healthcare. *Value in Health*, *19*(7), A705. doi:10.1016/j.jval.2016.09.2058.

[7] Bates, D. W., Saria, S., Ohno-Machado, L., Shah, A., & Escobar, G. (2014). Big Data In Health Care: Using Analytics To Identify And Manage High-Risk And High-Cost Patients. *Health Affairs*, *33*(7), 1123-1131. doi:10.1377/hlthaff.2014.0041.

[8] Bian, J., Topaloglu, U., & Yu, F. (2012). Towards large-scale twitter mining for drug-related adverse events. *Proceedings of the 2012 international workshop on Smart health and wellbeing - SHB '12*. doi:10.1145/2389707.2389713.

[9] Blair, L. M. (2016). Publicly available data and pediatric mental health: leveraging big data to answer big questions for children. *Journal of Pediatric Health Care*, *30*(1), 84-87. doi:10.1016/j.pedhc.2015.08.001

[10] Brewka, G. (1996). Artificial intelligence—a modern approach by Stuart Russell and Peter Norvig, prentice hall. series in artificial intelligence, Englewood Cliffs, NJ. *The Knowledge Engineering Review*, *11*(01), 78. doi:10.1017/s0269888900007724.

[11] Bryman, A., & Bell, E. (2011). *Business Research Methods* (3rd Revise). Oxford University Press.

[12] Bucherer, E., & Uckelmann, D. (2011). Business Models for the Internet of Things. *Architecting the Internet of Things*, (July), 253–277. http://doi.org/10.1007/978-3-642-19157-2.

[13] Cambridge Advanced Learner's Dictionary & Thesaurus. (2017). The internet of things. Retrieved February 16, 2017, fromhttp://dictionary.cambridge.org/dictionary/english/internet-of-things.

[14] Carman, K. L., Dardess, P., Maurer, M., Sofaer, S., Adams, K., Bechtel, C., & Sweeney, J. (2013). Patient and family engagement: a framework for understanding the elements and developing interventions and policies. *Health Affairs (Project Hope)*, *32*(2), 223–231. http://doi.org/10.1377/hlthaff.2012.1133.

[15] Cercone, F'IEEE, N. (2015). What's the big deal about big data? *Big Data and Information Analytics*, *1*(1), 31-79. doi:10.3934/bdia.2016.1.31.

[16] Chan, H. C. Y. (2015). Internet of things business models. *Journal of Service Science and Management*, *8*(4), 552.

[17] Chesbrough, H. (2010). Business model innovation: Opportunities and barriers. *Long Range Planning*, *43*(2–3), 354–363. http://doi.org/10.1016/j.lrp.2009.07.010.

[18] Chesbrough, H., & Rosenbloom, R. S. (2002). The role of the business model in capturing value from innovation : evidence from Xerox Corporation ' s technology spin-off companies. *Industrial and Corporate Change*, *11*(3), 529–555. http://doi.org/10.1093/icc/11.3.529.

[19] Christensen, C. M., Grossman, J. H., & Hwang, J. (2009). *The Innovator's Prescription: A Disruptive Solution for Health Care*. New York: McGraw-Hill.

[20] C.H.Daouk, L.A.EL-Esber and M.A.AL Alaoui (2002). IRIS Recognition. *Electrical and Computer Engineering*

Department, Faculty of Engineering and Architecture American University of Beirut. Retrieved from http://feaweb.aub.edu.lb/research/dsaf/Publications/25.pdf.

[21] Davenport, T. H., & Lucker, J. (2015). Running on data. *Deloitte Review*, (16), 5–15.

[22] De Cleyn, S., De Vos, K., Kallstenius, T., Van Bruystegem, E., Van Daele, W., & Vermeulen, S. (2015). Citizen health empowerment. *iMinds Insights*, 40. Retrieved from https://www.iminds.be/en/gain-insights/iminds-insights/citizen-health-empowerment 54.

[23] Deloitte. (2017). 2017 Global Health Care Outlook. Retrieved from https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/global-health-care-sector-outlook.html.

[24] Dhar, V. (2014). Big Data and Predictive Analytics in Health Care. *Big Data*, *2*(3), 113-116. doi:10.1089/big.2014.1525.

[25] Dul, J., & Hak, T. (2008). Case study methodology in business research (First edit). Elsevier. Ellinger, A. D., Watkins, K. E., & Marsick, V. J. (2005). Case study research methods. In R. A. Swanson & E. F. Holton (Eds.), Research in organizations: Foundations and methods of inquiry (First edit, pp. 327–350). Berrett-Koehler Publishers.

[26] European Commission. (2016). Protection of personal data. Retrieved May 1, 2017, from http://ec.europa.eu/justice/data-protection/

[27] Fleisch, E., Weinberger, M., & Wortmann, F. (2014). Business Models and the Internet of Things. *Bosch IoT Lab White Paper*, (SEPTEMBER), 19. http://doi.org/10.13140/RG.2.1.3824.2008.

[28] Gassmann, O., Frankenberger, K., & Csik, M. (2013). *The St . Gallen Business Model Navigator*. Retrieved from https://www.alexandria.unisg.ch/224941/1/St. Gallen Business Model Navigator.pdf.

[29] Geng, H. (2017). Internet of Things and Data Analytics Handbook. John Wiley & Sons.

[30] Gerkens, S., & Merkur, S. (2010). Belgium: Health system review. *Health Systems in Transition*, *12*(5), 1–266.

[31] Gong, A. (2013). Comment on "data science and its relationship to big data and data-driven decision making". *Big Data*, *1*(4), 194-194. doi:10.1089/big.2013.1514

[32] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. http://doi.org/10.1016/j.future.2013.01.010.

[33] He, D., & Zeadally, S. (2015). An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography, *2*(1), 72–83. http://doi.org/10.1109/JIOT.2014.2360121.

[34] Holler, J., Tsiatsis, V., Mulligan, C., Avesand, S., Karnouskos, S., & Boyle, D. (2014). *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*. Retrieved from http://store.elsevier.com/product.jsp?isbn=9780124076846.

[35] Hui Suo, Jaifu Wan And Caifeng Zou (2012). Security in the internet of Things: a review. International Conference, Hangzhou, China. Retrieved from http://ieeexplore.ieee.org/abstract/document/6188257/.

[36] J.Daugman (2004). How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*. Volume: 14, Issue: 1, Jan. 2004. Retrieved from http://ieeexplore.ieee.org/document/1262028/.

[37] Jie Lin, Wei Yu and Nan Zhang (2017). A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*. Volume: 4, Issue: 5, Oct. 2017. Retrieved from http://ieeexplore.ieee.org/document/7879243/.

[38] Johnson, M. W., Christensen, C. M., & Kagermann, H. (2008). Reinventing your business model. *Harvard Business Review*, *86*(12).

[39] Jorge Granjal, Edmundo Monterio and Jorge Sa Silva (2015). Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*. Volume: 17, Issue: 3, third quarter. Retrieved from http://ieeexplore.ieee.org/document/7005393/.

[40] Kaiser, L. S., & Lee, T. H. (2015). Turning Value-Based Health Care into a Real Business Model. *Harvard Business Review*, 1–5. Retrieved from https://hbr.org/2015/10/turning-value-based-health-care-into-a-real-business-model.

[41] Kranz, M. (2016). Building the Internet of Things Implement New Business Models, Disrupt Competitors, Transform Your Industry, Wiley.

[42] Ma, D. (2007). The Business Model of "Software-As-A-Service." *IEEE International Conference on Services Computing (SCC 2007)*, 701–702. http://doi.org/10.1109/SCC.2007.118

[43] Ma, D., & Seidmann, A. (2008). The Pricing Strategy Analysis for the "Software-as-a-Service" Business Model. In *International Workshop on Grid Economics and Business Models* (pp. 103–112). Las Palmas de Gran Canaria, Spain: Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-540-85485-2.

[44] Mahoney, B. (2012). Big earth 2014; big data! 2012 Conference on Intelligent Data Understanding. doi:10.1109/cidu.2012.6382180.

[45] Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). The Internet of Things: Mapping the value beyond the hype. *McKinsey Global Institute*, (June), 144.

[46] Marconi, K., Dobra, M., & Thompson, C. (2013). The use of big data in healthcare. Big Data and Business Analytics, 229-248. doi:10.1201/b14700-15

[47] Massa, L., Zott, C., & Amit, R. (2010). The business model: Theoretical roots, recent developments, and future research. *IESE Business School-University of Navarra*, 43.

[48] Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. *Nist Special Publication*, *145*, 7.

[49] Minerva, R., Biru, A., & Rotondi, D. (2015). IEEE- Towards a Definition of the Internet of Things (IoT).

[50] Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516. http://doi.org/10.1016/j.adhoc.2012.02.016.

[51] Morris, M., Schindehutte, M., & Allen, J. (2005). The entrepreneur's business model: Toward a unified perspective. *Journal of Business Research*, *58*(6), 726–735. http://doi.org/10.1016/j.jbusres.2003.11.001 56 .

[52] Raghupathi, W. (2010). Data Mining in Healthcare. *Healthcare Informatics*, 211-224. doi:10.1201/9781439809792-c11.

[53] Ripberger, J. T. (2011). Capturing Curiosity: Using Internet Search Trends to Measure Public Attentiveness. *Policy Studies Journal*, *39*(2), 239-259. doi:10.1111/j.1541-0072.2011.00406.x

[54] Ruths, D., & Pfeffer, J. (2014). Social media for large studies of behavior. *Science*, *346*(6213), 1063-1064. doi:10.1126/science.346.6213.1063.

[55] Sathish Ampalaya Kumar, Tyler Vealey and HarshitSrivastav (2016). Security in internet of things: challenges, solutions and future directions. *System Sciences (HICSS), 49th Hawaii International Conference, Koloa, HI, USA*. Retrieved from http://ieeexplore.ieee.org/document/7427903/.

[56] Saunders, M., Lewis, P., & Thornhill, A. (2015). *Research Methods for Business Students* (7th New ed). Pearson Education Limited.

[57] S.Barkathunishaan and R.Meenakumari (2013). Secure transmission of Medical Information using Iris Recognition. *International conference on ICCPEIC, Chennai, India*. Retrieved from http://ieeexplore.ieee.org/document/6778504/.

[58] Schatsky, D., & Trigunait, A. (2011). Internet of Things Dedicated networks and edge analytics will broaden adoption. *Deloitte University Press*, 307–323.

[59] Schellevis, J. (2014). Belgische rechter verbiedt taxi-app Uber in Brussel. Retrieved February 7, 2017, from https://tweakers.net/nieuws/95410/belgische-rechter-verbiedt-taxi-app-uber-in-brussel.html.

[60] Schilling, M. (2012). Strategic Management of Technological Innovation: Fourth Edition (Fourth). McGraw-Hill Higher Education.

[61] Schoen, H., Gayo-Avello, D., Takis Metaxas, P., Mustafaraj, E., Strohmaier, M., & Gloor, P. (2013). The power of prediction with social media. *Internet Research*, *23*(5), 528-543. doi:10.1108/intr-06-2013-0115.

[62] Sherin Zafar, M.K Soni and M.M.S Beg (2015). An optimized genetic stowed biometric approach to potent QOS in MANET. *International Conference on Soft computing and Software Engineering, SCSE 2015*.

[63] Sherin Zafar and M K Soni (2014). A novel crypt-biometric perception algorithm to protract security in MANET. *MR international Journal of Engineering and Technology, vol. 8, No.1, June 2014*.

[64] Shivaji Kulkarni , Shrihari Durg and Nalini Iyer 2016. Internet of Things (IoT) security. *3rd International Conference, (INDIACom), New Delhi India*. Retrieved from http://ieeexplore.ieee.org/document/7724379.

[65] Sinnott, R., Duan, H., & Sun, Y. (2016). A case study in big data analytics. *Big Data*, 357-388. doi:10.1016/b978-0-12-805394-2.00015-5.

[66] Steinbrook, R. (2008). Personally controlled online health data--the next big thing in medical care? *The New England Journal of Medicine*, *358*(16), 1653.

[67] Sweeney, L. (2002). k-anonymity: a model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(05), 557-570. doi:10.1142/s0218488502001648.

[68] Velthuis, E., Malka, E., & Richards, M. (2013). 'Big Data' in Health Care. What Does It Mean and Will It Make a Difference? *Value in Health*, *16*(7), A479. doi:10.1016/j.jval.2013.08.906

[69] Vermesan, O., Friess, P., Guillemin, P., Giaffreda, R., Grindvoll, H., Eisenhauer, M., … Tragos, E. Z. (2015). Internet of Things beyond the Hype : Research , Innovation and Deployment. *Building the Hyperconnected Society - IoT Research and Innovation Value Chains, Ecosystems and Markets*, 15–118.

[70] Viju Raghupathi, W. R. (2013). An overview of health analytics. *Journal of Health & Medical Informatics*, *04*(03). doi:10.4172/2157-7420.1000132.

[71] Walker, R. (2015). Impact of analytics and big data on corporate culture and recruitment. *From Big Data to Big Profits*, 184-201. doi:10.1093/acprof:oso/9780199378326.003.0009.

[72] Westerlund, M., Leminen, S., & Rajahonka, M. (2014). Designing Business Models for the Internet of Things. *Technology Innovation Management Review*, *4*(7), 5–14. Retrieved from http://timreview.ca/article/807.

[73] White, S. (2014). A review of big data in health care: challenges and opportunities. *Open Access Bioinformatics*, 13. doi:10.2147/oab.s50519.

[74] Wilkinson, Z. (2013). Oh, how pinteresting! an introduction to Pinterest. *Library Hi Tech News*, *30*(1), 1-4. doi:10.1108/07419051311320904.

[75] Yasseri, T., Sumi, R., & Kertész, J. (2012). Circadian patterns of wikipedia editorial activity: a demographic analysis. *PLoS ONE*, *7*(1), e30091. doi:10.1371/journal.pone.0030091.

[76] Yin, R. K. (2003). Case Study Research: Design and Methods. Applied Social Research Methods (Vol. 5). Sage publications.

[77] Yin, R. K. (2013). *Case study research: Design and methods* (5th Revise). Sage publications.

[78] Zembro. (2017). Zembro personenalarm. Retrieved May 1, 2017, from https://www.zembro.com/.

[79] Jorge Granjal, Edmundo Monterio and Jorge Sa Silva (2015). Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*. Volume: 17, Issue: 3, third quarter. Retrieved from http://ieeexplore.ieee.org/document/7005393/.