Contents lists available http://www.kinnaird.edu.pk/

Journal of Natural and Applied Sciences Pakistan

Journal homepage: http://jnasp.kinnaird.edu.pk/

EXTENUATING THE EFFECTS OF CYBER SECURITY IN INTERNET OF MEDICAL THINGS (IOMT)

Rimla Pervaiz[1], Washma Mir[1*], Sidra Anwar[1]
[1]Department of Computer Sciences, GC Women University, Sialkot.

Article Info

*Corresponding Author
Email: naseem1997@gmail.com

Abstract

Amidst of this chaos, where we say data is the most significant asset in every sphere and particularly if we put beam of attention on Internet of medical things which is dedicated to secure patient's electronic data is highly important. By knowing the fact that emphasizing a security check alone on data cannot resolve all emerging issue/challenges. Need to look more upon such techniques which will collectively lower data damage rate by uprooting different levels of security. The proposed healthcare security framework comprises different level of security based on information classification i.e.: from following the distinct approach of giving limited access on patient's data as per user's need and identity to counter security measures which is generating alerts to warn the user that someone's trying to access illegally on top of that providing security is the main aspect where cryptography plays a key role to ensure the security of all inter/intra systems, we aim in focusing not just on the secure transmission of data but also the safety of entire data residing by restricting the IP address of the system which will resultantly save data from plethora of issues and sub-issues i.e. Putting it to wrong use, data theft and so on.

Keywords

Electronic Patient Health Information (ePHI), Health Insurance Portability and Accountability Act (HIPAA), IoT (Internet of Things)

1. Introduction

The (IoT) Internet of Medical Things is a major medium for clinical tracking of illness owing comparitively low cost, private and reliable devices who don't need a very complex continuous integration. Recently, there is an urgent need to raise awareness in people/patients about sharing their sensitive medical information also to know about the potential needs that will eventually reducing the risk of losing or misusage of patient's information. Clinical development interoperability entails threats, pressures and obstacles but also risks. Stakeholders, clinical development clients, promoters and donors, medical trialists, and state regulators have major

concerns and priorities to be monologue and addressed at all times. However, the Iot Internet of Medical things is increasing fastly in the area of health treatment (Dimitrov, 2016).

Many of the advantages that IoT technology provides in the healthcare sector are mostly divided into monitoring patients, personnel, and items, recognizing, authenticating, persons, and automated data and sensing processing. Once patient movement is tracked, the procedure in the hospital may be greatly improved. In addition, verification and recognition eliminates accidents that may be detrimental to patients, record management and less instances of children who are not matched. Therefore, electronic data collection and delivery is essential in workflow integration, elimination of schedules for type production, automated surgical monitoring as well as medical optimization. Sensor devices enable patient-centered functions, in particular in the diagnosis of disorders and the provision of real-time information on health measures for patients (Zanjal *et al,* 2016).

Within this sector, technology areas include; being able to track a patient's adherence with prescriptions, telemedicine solutions, and patient well-being alerts. This requires devices to be added to ambulatory and inpatient patients, dental Bluetooth systems and tooth brushes that can provide details after use and patient monitoring. Many IoT items in this functionality include; RFID, Bluetooth, and, among others, Wi-Fi. These will greatly improve the assessment and control of vital functional strategies such as blood pressure, temperature, heart rate, blood glucose, glucose levels and others.

The Health Insurance Portability and Accountability Act 1996 (HIPAA) Protection Regulation includes ePHI leadership (McDaniel, 2009).

HIPAA Protection Rule sets out the following 3 forms of patient medical information:

- Info regarding "the history, long or short term physical or mental health or status of the person"
- Details on "the person's delivery of medical care"

Knowledge concerning "the previous, current or future compensation for the medical care service of the patient" With medical organizations moving quickly from traditional to digital records, introducing EHRs, and linking with HIEs, medical record’s solutions were also taken into consideration.

1.1.Issues of IOMT

- Hacking/Intrusion: Infringements of data by an unauthorized entity (i.e., a hacker) are what most people suspect when they learn about a data breach. This may escalate to phishing, ransomware/malware and skimming.
- Accidental Web/Internet Exposure: If someone links to some unknown network, Sensitive data is unintentionally put at a Web-accessible location. Through gaining

power over the network, any outsider may access the data.

- Data on the Move: Ensuring the transportation details is often a problem for companies. One common cause is the use of HTTP and other unreliable protocols. Each attacker is able to read it (active) although he can't alter it.
- Employee Error/Negligence/Improper Disposal/Lost: This term includes all data breaches due to negligence on the part of employees. Poor and/or poorly enforced data security measures may contribute to accidental breaches of the records.
- Insider Theft: This segment mostly deals with staff, which includes situations in which outsiders intentionally violate sensitive data.
- Physical Theft: Laptops and portable devices often hold useful or sensitive data. When taken into public areas such machines can easily get lost or robbed.
- Unauthorized Access: Poorly structured or enforced access controls may allow individuals to access information they are not allowed to access.

2. Background

The problem of securing the ePHI devices started when they started facing issues like Insider theft, Careless mistakes, Phishing attacks, Third party vendor risk, Oversharing, Employee error. Then it was handed over to HIPAA to cover these threats who worked on it thoroughly (Meingast *et al,* 2006).

To begin with the background of issues related to Health Information, a mid-sized hospital worker was distantly involved in a scandal after her husband got sued by a survivor (Bakker, 2007) of an accident. When the defendant at the facility went there, the staff member looked of the patient's data and gave her husband private information. The husband called for the defendant to dismiss the case. The defendant called the hospital and the office of the Attorney General to complain rapidly. If sentenced, the contractor faces a fine of $250,000 and up to 10 years in jail.

When a computer carrying thousands of patient health records was robbed from the parked vehicle, a heart monitoring company hit HIPAA warm water. The OCR has settled with the contractor for $2.5 million, showing government is really proactive, investigating HIPAA incidents involving outer theft and electronic attachable devices.

A HIPAA (OCR HIPAA Privacy, 2003) case may seem to come from nowhere in some instances, and avoiding it would demand a lot of creative thought from the employees of a clinic. In 2016, a physiotherapy hospital contyracted independent contractor to transform all X-Ray films in a paper form and then extract the silver from the films. This is an excellent example, as the hospital did not sign a business associate contract with the supplier first, it breached HIPAA. The hospital

was sentenced to pay $750,000 and adopt a *Preventative Recovery Plan.*

The effective way to avoid illegal snooping that breaches HIPAA, is to set up a process for detecting it. A Virginia hospital found 14 staff members who illegally handled a heavy-profile (Security Guidelines, 2006) patient's medical records. The hospital captured the staff members in the IT back end thanks to a mining system. The program monitors and documents all access to Patients Health Information documents. Fourteen staff members were removed from work. While this is commendable, (MedPro Disposal, 2017) a good approach could to notify staff members in advance that there is a tracking network, thus preventing breaches before hiring. And so on. Now if we talk about the main issues:

2.1.Data Breaches

Data breaches did not start when businesses started to store their data electronically. In fact, there have been data breaches as long as businesses and individuals preserve data and store personal information (Dolezel *et al,* 2019) . Once coding was normal, a data breach could be as easy as accessing the medical file (Zhang, 2020) of a person without permission or discovering confidential documents which were not easy to dispose of. Nonetheless, the rate of zdisclosed data breaches grew in the 1980s and public acceptance of the risk for data breaches started to increase in the 1990s and early 2000s (Palve *et al,* 2018) .There were 2,546 data breaches in medical care between 2009 and 2018 concerning 500 records. These thefts led in 189,945,874 health care records being theft / exposed. Which represents almost 59 percent of the U.S. population.

2.2.Insider Threats

Insider risks are not just workers, they can be suppliers, vendors, or volunteers who come into the company and work in it (Shaw, *et al,* 2011). Vormetric recently published the results of its 2015 Vormetric Insider Threat Survey, which showed that 92% of IT leaders thought that their companies were either relatively vulnerable to insider attacks, while 49% said that they considered somewhat or highly sensitive to internal threats. Among the most damaging examples of Insider Accusations was the (Procedure for third-party vendors and protected health information, 2018) cyber attack on state-owned oil organization Saudi Aramco, which deleted information from the company's business PCs using a virus called Shamoon on about 30,000 or three-quarters, and replaced it with a picture of a burning American flag.

2.3.Hacking

The term "cyberspace" was coined in the early 1980s from a story called "Neuromancer." A group named the "414s" is one of the earliest hacking groups ever to be attacked by the FBI and 60 device intrusions are charged. At such a time, Usenets started popping up around the country and hackers used their UNIX-based devices to share ideas (Campbell, 2018). At the age of 15, teen hacks NASA and the U.S. Department of

Defense. And for three weeks, NASA's system remained shut down. External partner access to your company can come in many shapes and forms (Spyd3r, 2002). Hackers are progressively targeting electronically protected medical information (ePHI), as they can get a high price on the black market (Ashiq, 2015) for this personal information. According to a Javelin Tactics & Research report, in 2016, 15.4 million customers were survivors of identification fraud or theft that cost more than $16 billion in U.S. customer

2.4.Largest Healthcare Data Breaches (2009-2018)

Department of Health and Human Services Office for Civil Rights started publishing summaries of healthcare data breaches, this is the brief analysis of healthcare data breaching from October 2009, when patient's sensitive data has been disclosed in an unauthorized manner to an untrusted environment (Healthcare data breach statistics, 2018).

Table 1: Brief Analysis of data breach (2018-2019)

Case No.	Names of Parties	Year	Covered Parties Type	People Impacted	Form of theft
i.	Anthem Inc.	2015	Healthcare Planning	78,800,000	Hacked
ii.	Premera Blue Cross	2015	Healthcare Planning	11,000,000	Hacked
iii.	Excellus Health Plan Inc.	2015	Healthcare Planning	10,000,000	Hacked
iv.	University of California, Los Angeles Health	2015	Medical-care Facilitator	4,500,000	Hacked
v.	Advocate Medical Group	2013	Medical-care Facilitator	4,029,530	Third party access
vi.	Banner Health	2016	Medical-care Facilitator	3,620,000	Hacked
vii.	21st Century Oncology	2016	Medical-care Facilitator	2,213,597	Hacked
viii.	Employees Retirement System of Texas	2018	Healthcare Planning	1,248,263	Unlicensed Access/Revealed
ix.	AvMed, Inc.	2010	Healthcare Planning	1,220,000	Third party access
x.	CareFirst BlueCross BlueShield	2015	Healthcare Planning	1,100,000	Hacked
xi.	Montana Department of Public Health & Human Services	2014	Healthcare Planning	1,062,509	Hacked
xii.	The Nemours Foundation	2011	Medical-care Facilitator	1,055,489	Lost

xiii.	BlueCross BlueShield of Tennessee, Inc.	2010	Healthcare Planning	1,023,209	Third party access
xiv.	Sutter Medical Foundation	2011	Medical-care Facilitator	943,434	Third party access
xv.	Valley Anesthesiology and Pain Consultants	2016	Medical-care Facilitator	882,590	Hacked

3. Related work

Released under the Health Information Technology for Economic and (Ni *et al*, 2017) Medical Health (HITECH) Act, the Interim Final Regulation for Unsecured PHI was released in the Final document on August 24, 2009 and came into effect on September 23, 2009. In contrast to those provided by the HIPAA Privacy Regulation, the Protection Policy criteria were discussed in detail in the "Policies and Procedures for UWM".

3.1.Cryptography

Nobody would say that cryptography and encryption are some new/alien tactics. This was true years ago and is still true, most trustworthy way to protect data is to encrypt it. Intelligence agencies and large financial institutions used cryptography and encryption (Goshwe, 2013) to defend their sensitive data for a long time. The study, co-sponsored by authentication technology provider, nCipher, "Authentication and Key Technology," showed that finest-in-class organizations (a classification that Aberdeen described as including organizations that saw the greatest change in their efficiency in IT protection over the past 12 months)(Kelly, 2009; Kaliski, 1993). EHRs is divided into a hierarchical system in which each portion is encrypted (Kaur, *et al,* 2014) with a modified public key to be handled by an authorized user and decrypted from a main private key with a modified sub key. The paper discusses many concerns: possible cost for access control, emergency services, and probable information retention problems because medical records are handled by suppliers of medical care. While several EMR and PHR solutions were developed, for cloud-based EHR solutions there is very little work (Alshehri, *et al,* 2012). Business cloud-based EHR solutions such as Performance Exchange and Support Cloud are reported to conform HIPAA, but their EHR protection is driven only on access control measures that are enforced by their google cloud suppliers.

EHRs is held unencrypted, with repercussions for privacy and security. PHR programs handle patient-imported private electronic medical records (Alshehri, *et al,* 2012) through EMR and EHR networks to enter a file, medical providers must decode the database entry in order to find the position and title of the document and the symmetric key. They will then ask the cloud computer for the encoded record and decrypt it using symmetric key. Also clinicians can be holders of EHRs under Narayan's model,

therefore this method may not be used for cloud-based HER (Bakker, 2004) schemes. HealthVault, a cloud-based Patients Health Record service offered by Microsoft and the shortly to be withdrawn Google Health service, both promise authentication through EHR transfer from patient to server and back, but they tend to be more likely to rely on adequate authentication and limit remote access instead of complete encryption in order to secure EHR data. Furthermore, in recent years, significant attention was paid to authenticating encrypted information maintained publicly or in the cloud, but our emphasis is on secure and efficient management of connections to cloud data.

3.2.Network Securing

The more popular online protected health information (ePHI) is, the more interest it gets from hackers as they get a high price on the deep web for this private information (Puthal, *et al*, 2016). In order to secure electronic protected health information (ePHI), we can limit the IP of our system from cybercriminals. Spoofing is a type of popular breach of protection known as a man in the middle (MITM) attack (Tanase, 2003). A hostile party intercepts a lawful contact between two pleasant parties in such assaults. The unauthorized controller then monitors the data stream and can delete or change the details received by one of the initial respondents (HealthITSecurity, 2017) without understanding whether the initial recipient or the receiver. An intruder can thus trick a target into providing false data by "spoofing" the initial sender's name, which the receiver probably trusts.

In the 1980s, the idea of IP spoofing (IP Address Restrictions) was addressed originally in scientific circles. It was mainly conceptual, though known for a long time, till Robert Morris, for whom son wrote the very first Online Worm, found a security vulnerability in the TCP protocol known as pattern forecast. In the TCP / IP Protocol Suite, (Harris, *et al*, 1999) a report that presented technical issues with the TCP / IP protocol suite, Stephen Bellovin explored the security issues in detail. A further iconic assault, the Christmas Day hole of Tsutomu Shimomura's device by Kevin Mitnick, used the forecast strategies for IP spoofing and TCP series. While the prevalence of such loopholes has declined due to the collapse of the systems they abused, spoofing could still be used by all network managers and needs to be tackled. The Protection Rule provides processes to protect ("EPHI") and stop unapproved persons from accessing such sensitive information. EPHI (Smid, *et al*, 1988) is specified by Protection Law as ("PHI") processed or distributed through digital media. Control systems should be as isolated as possible for network devices. Control interfaces should be mounted on separate Ethernets, separate VLANs, using unrouted IP addresses of RFC 1918, and use serial links to a specific admin console The network must be on a domain controller that the general population can not reach. In this scope, IP addresses must only be available to the

operational authorities of the UITS or any other IT staff supporting the Covered Agency.

3.3.Data Filtration and Classification

Over time, the classification of data has improved substantially. Currently, for a different purpose, the software is used, often in help of data security initiatives. But for a couple of reasons, information can be categorized, including ease of access, retaining risk management, and achieving various other business or personal goals. Data classification is a valid tactic for data protection methods, which facilitates appropriate security reactions based on the type of data being recovered, transferred, or reproduced (Botsis, *et al,* 2010). A carefully designed information filtering (Facer, *DISPLAYR Blog)* system also makes it easier to manage and monitor important data as well as making it easier to find and manage data. While some variation of all the following features can be accomplished, when approaching a data classification (Tech Target: Search Data Management, 2019) initiative, most businesses and data experts concentrate on a specific goal (Weber, *et al,* 2017). The most common goals and objectives are the following, but not restricted to:

- **Confidentiality.** A classification process above other features that values secrecy will concentrate mostly on security protocols, including client authorizations and authentication.
- **Integrity of data.** A data integrity-focused framework would need more space, user access, and correct access networks.
- **Availability of data.** While protection and honesty need not be mastered, making information easier for users to access.

3.4.Data classification

Is a way to secure compliance with organization, local or federal data managing procedures and a way to maintain and optimize data protection. The use of data classification (Olzak, 2007) enables agencies to maintain their data's privacy, accessibility and dignity. It also minimizes the risk of hackers being exposed to informal confidential information and protects companies from high data storage expenses. It is costly and may also be a burden to store huge amounts of disorganized data (Hardy, 2017) .

3.5.Monitoring and Reporting

A tool for offering real-time support in evaluating patient records data and tracking parameters obtained from a patient to determine possibilities and background of care for the patient based on previous patients with similar monitoring parameters and health record data. The system consists an integrated control software which obtains patient tracking parameters and interacts with a historical database of references that includes numerous historical records of patients.The traditional reference list recognizes one or more existing medical records that closely resemble the patient being monitored after obtaining the patient's tracking criteria and

medical records (Rahman, *et al,* 2016). Based on actual records of patients detected, the alert is produced on the basis of the information in real time.

Security issue notification is distinct from the Breach Notification Standard (below) in so far as it is possible to identify accidents and to collect data before the incident evolves into a breach. Real-time alerts can trigger alert actions on a per-result basis. They can also trigger alert actions when results meet user-defined conditions within a rolling time window. For hospitals or urgent care settings, there is a massive shift in care to personal areas like the family of the (Pendergast, *et al,* 2007) patient, wherever possible. It is predicted that the worldwide smart health industry will reach $169.30 billion through 2020 with a famous health monitoring task (Technavio)..

4. Frame Work

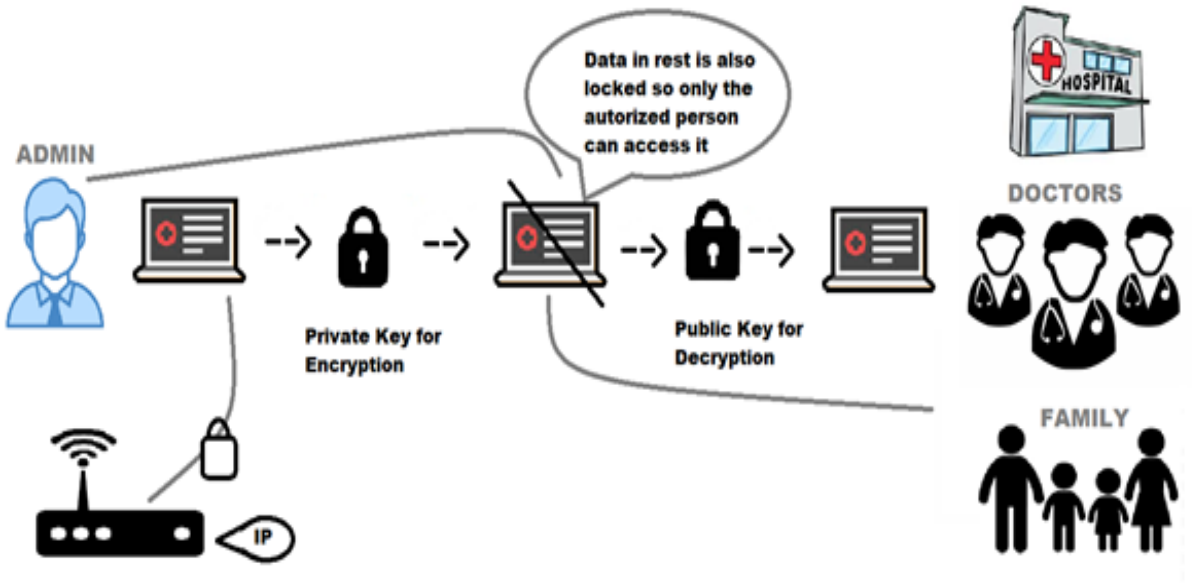

Figure 1: Security of whole

Figure shows how this paper is securing the medical records in all fields. Data of patients will be secured during transferring, IP is also secure, Data in rest is also secure and the access to every authenticated person is also limited.

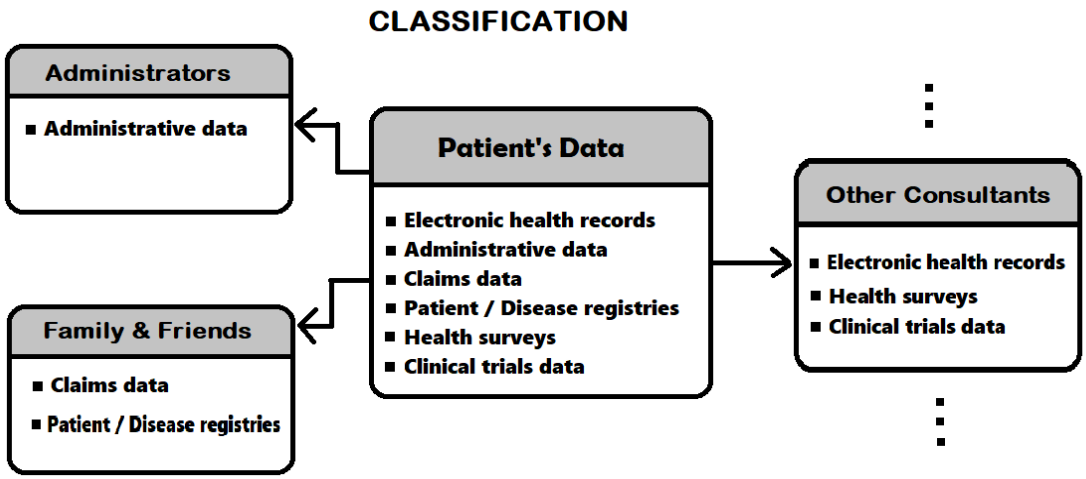

Figure 2: The way data of patient's is going to be classified for different authentic accesses.

5. Analysis

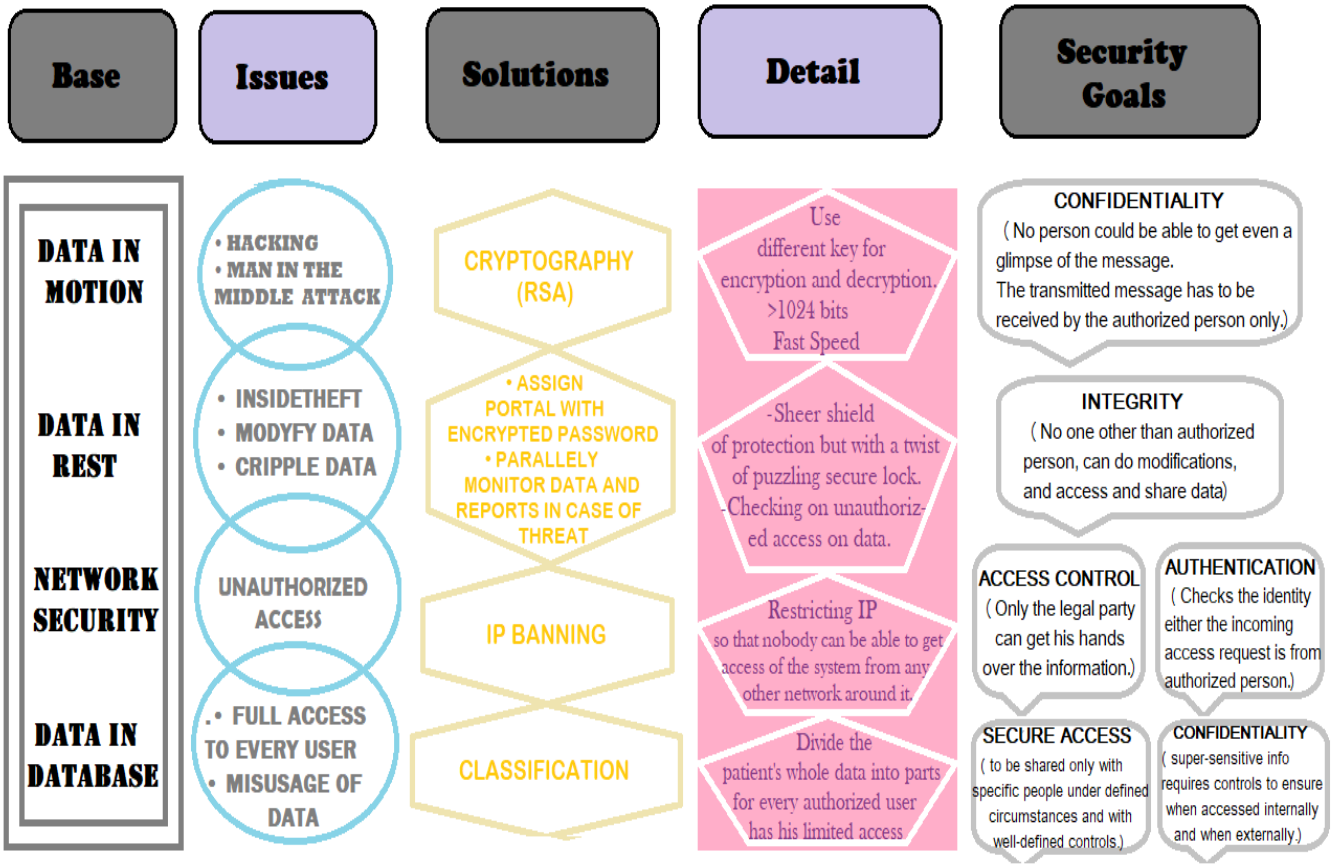

Figure 3: Analysis based on different issues of security.

This diagram contains amalgam of techniques with the precise review that how they eventually work and how this paper is achieving security goals by minimizing all the security threats to ePHI.

6. Discussion

As now more and more hospitals leaning upon saving their data electronically and massive amount of patient's data is being saved /transferred, ironically there comes a more need to overcome the issue of securing ephi, which is getting serious every day. The higher the usage, the more you seeding risks. Such as hacking, insider theft, data breaching and so much more issues like these outburst the hunger of using more technology like cryptography to resolve them.

Securing ephi is our main agenda but for it we need to identify what is our goal and what footsteps we need to follow to achieve it.

- This paper is merging different aspects of security and providing a brief model.
  a) Starting from the classification of given data, where patients' data will be organized. This will not only provide ease in locating data but also access controlling

by dispensing the unnecessary data while giving access to the authorized user as per his needs. While putting it in order, it'll also monitor the information.

b) After absorbing the information, it'll generate alert that will be according to the sensitivity of that information. while transmitting the data by key pair technique Cryptography is the need of the hour but with amendments in it according to our needs and requirements, when the data is in rest by generating logins of users and also banning IP address as Data security is just not possible without secure network, what you will do if the network of your system is not secure all the efforts will vigorously go in vain, to prevent it from outsider thefts.

7. Conclusion

Electronic Patient Health Records (EPHI) for doctors and patients is deemed private. The use of internet for file sharing by medical personnel may present privacy threats and non-compliance problems for health care providers. As the connectivity and usage of medical devices is increasing, there's a quick need of implementing an effective approach to assure a secure management system for patient's health information. Keeping this thing in mind HIPAA has established great rules for the patient's privacy, for everyone to follow. This paper "extenuating the effects of cyber security in IOT " has intended to settle the growth of some security issues, by providing a model as a competent security package including all inter and intra relation security, Network connectivity security, Classification and Monitoring, so that the patients can focus on their health rather than worrying about their personal information being disclosed.

This paper intends to reduce the risk for IoT medical by providing end to end security by using cryptography key pair technique and securing the network connection by banning IP mainly.This paper provides a comprehensive healthcare IoT and cloud computing architecture which facilitates applications using the lead of IoT and cloud computing and provides a platform for enabling medical data sharing between medical devices and access of databases or cloud computing systems. But still there's a-lot of work to be done in this field, by covering more security issues to enhance the proposed model one can reduce more obstacles in the way of secure PHI.

References

Alshehri, S., Radziszowski, S. P., & Raj, R. K. (2012). Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption. In *IEEE 28th International Conference on Data Engineering Workshops. Arlington, VA.* doi: 10.1109/ICDEW.2012.68

Ashiq, J.A. (2015). Insider vs. Outsider threats: identify and prevent. Retrieved from https://resources.infosecinstitute.com/ins

ider-vs-outsider-threats-identify-and-prevent/#gref

Bakker, A. (2004). Access to EHR and access control at a moment in the past: a discussion of the need and an exploration of the consequences. *International Journal of Medical Informatics,* 73(3), 267–270. doi:10.1016/j.ijmedinf.2003.11.008

Bakker, A. R. (2007). The need to know the history of the use of digital patient data, in particular the EHR. *International Journal of Medical Informatics,* 76(5-6), 438–441. doi:10.1016/j.ijmedinf.2006.09.009

Botsis, T., Hartvigsen, G., Chen, F., & Weng, C. (2010). Secondary use of EHR: data quality issues and informatics opportunities. *Summit on translational bioinformatics,* 1–5. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3041534/

Campbell, J. (2018). Risks associated with third-party access security processes to implement when dealing with third-party access to your company's network. *CSO from IDG Communications.* Retrieved from https://www.csoonline.com/article/3294707/risks-associated-with-third-party-access.html

Dimitrov, D.V. (2016). Medical internet of things and big data in healthcare. *Healthcare Informatics Research,* 22 (3), 156-63. doi: 10.4258/hir.2016.22.3.156

Dolezel, D., & McLeod, A. (2019). Big data analytics in healthcare: investigating the diffusion of innovation. *Perspectives in health information management, 16*(Summer), 1a.

Facer, C. What-is-data-filtering. *DISPLAYR Blog.* Retrieved from https://www.displayr.com/what-is-data-filtering/

Goshwe, N. Y. (2013). Data encryption and decryption using RSA algorithm in a network environment. *IJCSNS International Journal of Computer Science and Network Security*,13(7), 9-13. Retrieved from http://paper.ijcsns.org/07_book/201307/20130702.pdf

Hardy, J. (2017). What qualifies as EPHI According to HIPAA? More than you may think. *Affinity TECHNOLOGY PARTNERS.* Retrieved from https://www.affinitytechpartners.com/3n1blog/2016/7/21/what-qualifies-as-ephi-according-to-hipaa-more-than-you-may-think-

Harris, B., & Hunt, R. (1999). TCP/IP security threats and attack methods. *Computer Communications,* 22(10), 885–897. doi: 10.1016/S0140-3664(99)00064-X

Healthcare data breach statistics. (2018). Retrieved from

https://www.hipaajournal.com/healthcare-data-breach-statistics/

HealthITSecurity. (2017). *Security patches critical in ransomware prevention measures*. Retrieved from https://webcache.googleusercontent.com/search?q=cache:RdW48RndVoUJ:https://healthitsecurity.com/news/security-patches-critical-in-ransomware-prevention-measures+&cd=1&hl=en&ct=clnk&gl=pk

IP Address Restrictions. Paper Thin: Web Content & Experience Management. Retrieved from https://www.paperthin.com/products/features/ip-address-restrictions.cfm

Kaliski, B. (1993). A survey of encryption standards. In *IEEE Micro,* 13(6), 74-81. doi: 10.1109/40.248057.

Kaur, J.P., & Kaur, R. (2014). Security issues and use of cryptography in cloud computing. Retrieved from https://www.semanticscholar.org/paper/Security-Issues-and-Use-of-Cryptography-in-Cloud-Kaur Kaur/b23d7935a270b241bc5bf002e8f3a4d74f30901f

Kelly, M. D. (2009). A mathematical history of the ubiquitous cryptological algorithm. Retrieved from https://www.sccs.swarthmore.edu/users/10/mkelly1/rsa.pdf

McDaniel, J. (2009). Developing an information security program for HIPAA compliance. In *InfoSecCD '09: 2009 Information Security Curriculum Development Conference, Kennesaw Georgia*. doi: 10.1145/1940976.1940997

MedPro Disposal. (2017). 20 catastrophic HIPAA violation cases to open your eyes. Retrieved from https://www.medprodisposal.com/hipaa/20-catastrophic-hipaa-violation-cases-to-open-your-eyes/

Meingast, M., Roosta, T., & Sastry, S. (2006). Security and privacy issues with health care information technology. In *International Conference of the IEEE Engineering in Medicine and Biology Society, New York, NY.* doi: 10.1109/IEMBS.2006.260060

Ni, J., Zhang, K., Lin, X., & Shen, X. (2017). Securing fog computing for internet of things applications: Challenges and solutions. In *IEEE Communications Surveys & Tutorials,* 20 (1), 601-628. doi: 10.1109/COMST.2017.2762345

OCR HIPAA Privacy. (2003). A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. Retrieved from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/research/research.pdf

Olzak, T. (2007). Improve data protection processes with content discovery, monitoring and filtering. Retrieved from https://adventuresinsecurity.com/Papers/CMF.pdf

Palve, A., & Patel, H. (2018). Towards securing real time data in IoMT environment. In *8th International Conference on Communication Systems and Network Technologies (CSNT),* Bhopal, India. doi: 10.1109/CSNT.2018.8820213

Pendergast, J. & Brodnick, D. (2007). Case based outcome prediction in a real-time monitoring system. US20070244724A1. The General Electric Company, New York. United States

Procedure for third-party vendors and protected health information. (2018). *Information Technology, Research and Clinical Data Access, UMass Medical School.* Retrieved from https://www.umassmed.edu/it/security/research-and-clinical-data-access/standard-operating-procedure-for-third-party-vendors-and-protected-health-information/

Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2016). Threats to networking cloud and edge datacenters in the internet of things. In *IEEE Cloud Computing,* 3(3), 64–71. doi: 10.1109/MCC.2016.63

Rahman, M.M., Akter, T., & Rahman, A. (2016). Development of cryptography-based secure messaging system. *Journal of Telecommunications System & Management,* ISSN: 2167-0919. doi: 10.4172/2167-0919.1000142

Security Guidelines. (2006). *Health insurance portability and accountability act (HIPAA).* Retrieved from https://uwm.edu/hipaa/security-guidelines/

Shaw, E. D., & Stock, H. V. (2011). Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall. *IMG, Incident Management Group.* Retrieved from http://zadereyko.info/downloads/Malicious_Insider.pdf

Smid, M. E., & Branstad, D. K. (1988). Data encryption standard: past and future. In *Proceedings of the IEEE,* 76, (5), 550-559. doi: 10.1109/5.4441

Spyd3r. (2002). History of hacking. *+HELPNETSECURITY.* Retrieved from https://www.helpnetsecurity.com/2002/04/08/the-history-of-hacking/

Tanase. M. (2003). IP Spoofing: An Introduction. *India Documents.* Retrieved from https://fdocuments.in/document/ip-spoofing-an-introduction.html

Tech Target: Search Data Management (2019). What is data classification and why is it important? Retrieved from https://searchdatamanagement.techtarget.com/definition/data-classification

Weber, G.M., Adams, W. G., Bernstam, E.V., Bickel, J.P., Fox, K.P., Marsolo, K., Raghavan,V.A., Turchin, A., Zhou, X., Murphy,S.N., & Mandl, K.D. (2017). Biases introduced by filtering electronic health records for patients with "complete data", *Journal of the American Medical Informatics Association,* 24(6), 1134-1141. Retrieved from https://scholar.harvard.edu/weber/publications/biases-introduced-filtering-electronic-health-records-patients-complete-data

Zanjal, S. V., & Talmale, G. R. (2016). Medicine reminder and monitoring system for secure health using iot. In *Physics Procedia*, 78, 471–476. Elsevier B.V. doi: 10.1016/j.procs.2016.02.090

Zhang. E. (2020). What is data loss prevention (dlp)? A definition of data loss prevention. *DATAINSIDER Digital Guardian's Blog.* Retrieved from https://digitalguardian.com/dskb/data-loss-prevention