Health Data Security: A Privacy-Preserving Proposed Strategy for Bangladesh

A K M Bahalul Haque
Department of Computer Science and Engineering, North South University, Dhaka 1229, Bangladesh
bahalul.haque@northsouth.edu

Tahmid Hasan Pranto
Department of Computer Science and Engineering, North South University, Dhaka 1229, Bangladesh
tahmid.pranto@northsouth.edu

Abstract – Patient's data are too personal and sensitive that a person may never want to disclose. So, maintaining the privacy of these data and ensuring proper security and protection measurements should be given paramount importance. Many countries across the world, force the hospitals and healthcare organizations to maintain all this by imposing data privacy laws where many countries have specific laws or acts only for healthcare data. Bangladesh lacks a data protection law let alone healthcare data law that should have been already imposed as there is a clear need for that. In this paper we analyzed the healthcare situation of Bangladesh and prepared a threat model specialized for hospital or healthcare organizations. We proposed a strategy to address healthcare data security that starts with patient data collection and covers storage strategies, data flow architecture, data process mechanism and level of authority of data owners. We also proposed a chain of maintenance through continual testing and auditing. All these strategies and security measurements can be added to legislation for ensuring privacy, protection and security of healthcare data.

Index Terms – Data Security, Healthcare Data, Data Protection, Privacy Strategy.

1. INTRODUCTION

We are living in a world of automation and technological advancement where each and every step of our daily activity is creating data. Due to the immense development of cloud storage systems, the custom in storing information has changed radically. Paper based information storage is rarely seen in organizations these days. In accordance with technology, the health sector across the world has also adopted Electronic Patient Record Systems (EPRS) shifting from paper-based prescription or record keeping systems.

The rapid growth of digitization in Bangladesh healthcare industry has changed the scenario of patient care while imposing major threat against the privacy, security and protection of personal healthcare data. A large number of hospitals and healthcare organizations have adopted electronic means of patient data recording systems (EPRS) In Bangladesh. The government hospitals are also using EPRS to some extend and all the necessary steps to adopt full-fledged EPRS has also been implemented. But in developing countries like Bangladesh, large scale of healthcare data is under vulnerability threat due to proper education and consent of the patients. In addition to that, not having any data privacy, protection and security policy is alarming while this vast population of Bangladesh without any doubt produces immense volume of patient data. Without a proper policy, organizations and hospitals don't have proper rigidity regarding the privacy, protection and security of these data. On the other hand, collection, storage, process and inter organization sharing of patient data is necessary in the field of research, pharmaceuticals, health insurances and the hospitals themselves might also use data to upgrade quality of patient care.

Healthcare is a big industry consisting of hospitals, organizations, pharmaceuticals and the government itself. The data generated in the healthcare sector in terms of variety, velocity and volume has gone past the definition or regular data and falls under the category of big data. A recent report by IDC and the research by EMC shows that healthcare data increases by 48% per year. [1] In 2013 the amount of medical data was 153 exabytes where in 2020 the amount is expected to be 2314 exabytes. [1]

During admission or checkup appointments, many personal information is collected from the patient. On the other hand, the adoption of automated and advanced monitoring devices has enabled us to collect data every second. This data is not only stored for future use or record keeping purposes but also processed for a vast range of insight finding activities like improving the effectiveness of medicine, patient care activities, clinical decision and support management, disease surveillance and optimization of treatment procedure. These data of patients are also used by many organizations like health insurance companies, pharmaceutical companies, healthcare organizations, drug administration and by the government too.

But, invoking someone's privacy without proper consent of that subjected person is a serious punishable crime in many well-developed countries. Data can be sophisticated and, in some cases, too private to a person which he will never want to disclose to anyone which is called sensitive personal data. This very idea generated the thought of data privacy, protection and security which has been in talk for the past few decades. Many countries have laws to secure personal data privacy and to protect the data. For example, countries inside European Union follow the General Data Protection Regulation (GDPR) [2], Canada follows the Personal Health Information Protection Act (PHIPA) [3], and the United States has the Health Insurance Portability and Accountability Act of 1996 (HIPAA). [4] Healthcare data are rather sophisticated and personal to a patient than regular data. So, privacy of this data is a big concern.

Although digitization has been adopted in almost every sector of Bangladesh, no data protection or security law has been there since the independence of this country. According to Bangladesh Telecommunication Regulatory Commission (BTRC), there are 165.615 Million mobile phone users at the end of January [5], 2020 and a total of 100 million internet users till February,2020 in Bangladesh. [6] This huge number of populations having devices and internet connection is connected with one or many healthcare organizations and sharing data frequently without having proper knowledge about the privacy, safety and security of their personal data.

Apart from the discussed importance above, the major contribution of this work is to state the current condition of privacy, protection and security of healthcare data while establishing the necessity of taking proper measurements in the perspective of Bangladesh. This work also manifests the proper system and threat modeling to ensure better security. The summary of the paper can be specified as below.

- Current scenario discussion of country-based laws and acts.
- Bangladesh is setting its way to implement fully electronic patient record system.
- Necessity of protection, privacy and security of the healthcare data and proposed strategies.
- Detailed threat modeling and a proposed data flow structure.
- Future research directions in this sector.

In this paper section 2 establishes the fact that Bangladesh is adopting electronic patient record systems soon, without having any law for the privacy and protection of this huge healthcare data. Section 2 has the discussion about the related works that have been done in this area of research. Section 4 showcases the laws and acts across the world regarding healthcare data privacy, security and protection. After that, section 5 has a detailed discussion about the strategies to follow while collecting and processing while also discussing the strategies after storing the data. In section 6, possible threats for the system have been discussed and a solution threat model has been proposed followed by the future research directions in section 7.

2. DIGITIZING BANGLADESH HEALTHCARE SECTOR: CURRENT SITUATION

According to the Report on Bangladesh Sample Vital Statistics 2018 by the Bauru of Statistics Bangladesh, the population of Bangladesh is 164.4 million. [7] For this 164.4 million people there are 612 government hospitals and 5058 non-government hospitals, making it a total of 5666 hospitals. [8] On the other hand, this huge number of populations surely generates a large number of patients too. According to the live database of Bangladesh Directorate General of Health Services (DGHS), 9223372036854 billion OPD patients were reported in the last 12 Months across Bangladesh. [9] This immense number of patients across the country is generating data every second around the clock. From a paper-based healthcare record system, Bangladesh is moving forward to implement Electronic Patient Data Record System (EPDRS) in near future. Some movement towards digitizing the healthcare sector has already taken place.

According to the most recent “Annual Report HSD 2018-2019” [8] by the Ministry of Health and Family Welfare Bangladesh, 5702 desktops, 14000 laptops and 19700 tablets have been distributed in the 2018-2019 economic year to digitize the health sector. According to section 9.2 of HSD, more than 13 thousand community clinics in rural areas have been bought under internet connection and 24 thousand community clinic workers have been given a tablet computer with working internet connection (HSD Section 9.2 Subsection 1). [8] Every office of civil surgeons has been bought under LAN connection and is instructed to update health data time to time. 94 hospitals are connected in a software-based video conferencing system to ensure instant healthcare (HSD Section 9.2 Subsection 2). By doing so, the government is taking data from a very root level. Not only that but also for collecting data from all hospitals, OpenMRS software is instructed to be installed. (HSD Section 9.2 Subsection 9) [8]

Although there is not any national healthcare database, but all this data is being generated and recorded from a very root level. Privacy, protection and Security is a big concern if the workers and the whole system is not bought under a data privacy policy with clear and transparent instructions.

3. RELATED WORK

The protection of ones’ personal data is a basic human right whether it is stated legislatively or not. Especially, data related to healthcare can be more sophisticated and distinctive to a person. However, keeping, processing and analyzing healthcare data is required to improve treatment methods, and reduce costs. Processing these data has transformed the quality of service, improved the efficiency of clinicians, optimized treatment, improved health insurance schemes and also improved the perfection and effectiveness of medicines. [10,11] For example, Indiana Health Information Exchange connects 117 hospitals and they process more than 13 Billion clinical data elements to improve the standard of healthcare services. [12]

Improvement of technology, digitizing the workflow in healthcare and switching the record keeping systems to electronic versions, a great threat toward data privacy, protection and security has been introduced. In addition to that, sophistication in malware and security threats is increasing the challenges to keep data private, safe and secure. [13] There is also a great risk associated with the technologies that have been adopted by healthcare organizations. Production of sensitive information has increased by the growing trends like mobility of the clinicians, wireless networking, increasing exchange of healthcare information, cloud computing, use of Personal Health Record (PHRs) systems. [13]

The amount of data produced by the healthcare organizations in terms of volume, variety and velocity indicates the creation of “big data”. [11] Big data is large and complex sets of data that are difficult to manage, process and safeguard. This vast amount of data needs newer technologies to be protected and secured which has also become a basic requirement in healthcare sectors. [13] While the automations have led to improved patient care workflow and reduced costs, it is also rising healthcare data to increased probability of security and privacy breaches. According to Black Book research, over 96% of healthcare organizations have experienced a data breach of some kind over the past five years. [14] Data breach not only harms the right of personal privacy, but also brings economical damage to organizations. According to IBM’s Cost of a Data Breach [15] study, an average data breach can cost up to $3.9 million.

Controlling authentication, authorization, applying encryption methods, using data masking and controlling should be the center of designing healthcare management systems. [11] Privacy should be the default option for a patient and the system design of a healthcare organization must comply with that. Strategies like minimizing, hiding, separating, abstraction, inform, control and enforce should be applied to healthcare systems for ensuring “Privacy by Design” (PBD) [16].

While transferring data, proper anonymization must be ensured. De-identification techniques like k-anonymity, l-diversity, t-closeness, Hybrx must be applied to data so that the identity of an individual does not get exposed. [11]

To protect the privacy of the user and secure the data that is being taken and stored, a jointly working system has to be carried out where government imposed standardized legislative laws will protect the data and sturdy systems used in healthcare organizations will keep the data safe and secured.

4. HEALTHCARE DATA PROTECTION LAWS AND ACTS IN VARIOUS COUNTRIES

Name of The Law	Key Features
General Data Protection Regulation (GDPR), European Union	Most effective and practical law till date. This full featured law has 11 chapters and 99 articles. Gives full ownership of the data to the subject. Has legislations for every purpose of data usage. From organizational data process to inter-country data exchange, all is covered under GDPR. [2]
Personal Health Information Protection Act (PHIPA), Ontario,2004, Canada	There are a total 7 sections on this act. Section -2 discusses the practices to protect healthcare information, section-3 discusses the consent concerning personal health information, section-4 talks about the collection, use and disclosure of personal health information and section-6 has a brief information about the enforcement of these laws. [3]
Personally-Controlled Electronic Health Records Act, 2012, Australia	This is a complimentary act of Privacy Act 1988 [17] that is especially focused on the privacy and protection of healthcare data. In this act, Part-3 is about the registration procedures of patients, part-4 discusses collection, use and disclosure of patients’ data, part-4 discusses the legislative penalties of data abuse. The other sections discuss the need for this act and the civil rights of a patient. Section (1,2) clearly states that, it is forbidden to share data even with court or tribunal without the consent of the patient.[18]
Health Insurance Portability and Accountability Act of 1996 (HIPAA), USA	HIPAA applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form. [4] This law covers all the areas ranging from what data is to be protected, how to be collected and how to implement safety measurement in data storage. HIPAA includes serious penalty for data abuse that could range from 100$ to 50,000$ per violation.[4]
Health Information Technology for	Subtitle D of this act addresses the privacy and security concerns

Economic and Clinical Health (HITEC), 2009, USA	associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules. Section 13410 (d) of this act establishes a penalty amount of 1.5m$ for an identical provision. [19]
Health Information Privacy Code, 1994, New Zealand	Applies to all healthcare agencies who collect, store and process healthcare data. Rule 12 of this act allows direct complaint to the Privacy Commissioner in case of data breach or data abuse. [20]
Patient Data Act, (2008:355), Sweden	This act has law for every aspect ranging from collection to breach of healthcare data, that includes the limitation of data disclosure stated in Section-2(Law 2010:677). [21]
Health Data Law, Federal Law No 2 of 2019, UAE	This law applies to all agencies related to healthcare across UAE who use information technology and communication systems. The law establishes principles like limitation, accuracy, consent to disclosure and security measurement for healthcare data. It allows a data retention of 25 years on lawful purpose. The disciplinary sanctions range from warning to 1 million fines while taking away the license. [22]
Data Protection Act, 2018, UK	A seven-part act that covers data protection for general purposes as well as security and intelligence data process. The act includes six data protection principles that have to be followed. In case of data abuse, legislative penalties are covered under subsection (4,5), section (119, 170, 179, 184). [23]
Act on the Protection of Personal Information, 2017, Japan	A fourteen-section act to apply legislative laws on personal data acquisition, retention, use or handling. Has clear and separate laws for personal, specific personal, sensitive and anonymized personal data. [24]

Table 1: Data Protection Laws Around the World

5. PROPOSED DATA PRIVACY AND PROTECTION STRATEGY

5.1. Data Collection

In general, a great extent of information is counted as data like car license no, passport no, bank account no, personal identification information or even a person's geological location. But the healthcare sector works with some specific types of data which is supposed to be related with treatment or identifying the patient. A common norm in medical data collection is by asking and gathering. Some official stuff asks whatever information the hospital needs and records them using some kind of Electronic Patient Record System (EPRS).

But medical data is often too personal or sensitive for patients. Data like name, address, height, weight, heart rate, blood group or heart rate are common personal data but in hospitals, some very sensitive information is often needed for treatment purposes. Data like sexual preference, infectious disease or infertility has to be kept as private as possible because no person would like to disclose or discuss this data publicly.

The flow of patients' data throughout the system, starts with collection of data. After the collection and entry, then the data gets stored in the storage system. Precautions should be taken to ensure the privacy, protection and security of this data from the very beginning. People generally come to the hospital with their previous prescriptions and other documents. While inserting a new patient in the EPRS, this below policies should be maintained.

Every patient will have a uniquely identifiable number. To avoid generation of separate id's for patients pre-existing verified identification numbers can be used like national id no, passport no or birth certificate. This personal identification number must be associated with patients' information.

Whenever in the treatment process data is needed to be taken from the patients, official stuffs will provide leaflets that discusses the followings in a simple, non-technical and human readable form:

I. Relevance: Why the data is being taken or why it is related to the treatment process.

II. Collection Method: How the data will be collected.

III. Data process: How the hospital processes data. Do they share it to other organizations or with the government?

IV. Safety Measurements: A small discussion of how safe the patient should feel about their data. The data safety measurements taken by the hospital or organization.

After the patient knows about the data sharing relevance, security and process, he/she should be given a consent form that will work as a contract between the organization and the patient. The patient will sign the consent. In case of children or senior citizens or seriously ill people, a close attendee will sign on behalf (e.g. Parents, Children, Wife, Siblings).

Authorized persons will only do data collection. That might include senior nurses in the pre-checkup room, staff at the registrar desk and the doctors.

During the data collection, the data collection authority must log into the system with proper credentials. In this case OTP (one-time password) or two factor authentications can be used to cross check the validity of the credential.

Sensitive personal data must be collected either by written form or in a separate cabin.

5.2. Data Processing

After the successful collection of data, it needs to be stored in the storage system. But before storing, some precautions must be taken for the sake of ensuring privacy, protection and safety of those data. We propose a separate database for personal data and healthcare data. Right after the data has been taken primarily by the collection staff or doctors, data will be handed over to a controlling and processing team (CAP) consisting of technically trained persons. Only the control and processing team will have the authority to process any data before it goes to the database. The strategies or steps below should be followed by the CAP team.

5.2.1. Authority to Store

Only the CAP team will be responsible for conducting the activities related to storing the data while maintaining proper technological security and protection measurements.

5.2.2. Separation of Data

They will separate the data into two categories based on sensitivity of the data. The categories are:

I. Personal Data: Only personal data like name, id, address, appointment information and billings will be there under personal data category.

II. Health Data: Along with the personally recognizable id, only health information like laboratory reports, operation information or doctor’s prescription will be there under this category.

5.2.3. Patient Data Encryption

The CAP team will apply cryptography methods along with all the implementation of necessary algorithms to safeguard the data within the system. They will generate ‘keys’ along with some suitable algorithm(‘cipher’) to generate the ciphertext and instead of direct data, those ciphertexts will be stored in the storage used by the hospital. They will also make sure that the data is encrypted at rest (when data is in the storage and not being accessed) and at transit (when data is being retrieved). A possible encryption method is homomorphic encryption. It allows mathematical operation on ciphertexts. An encrypted ciphertext along with some mathematical operation on it is safer to be stored. Another advantage of homomorphic encryption is data sharing. Any kind of analytics or research work can be done on ciphertexts encrypted using a homomorphic encryption method.

5.2.4. Encrypting Communication

For operations like chats between doctor and patient, data must be secured with end to end (E2E) encryption as it can contain very sensitive private data. Using cryptographic techniques, only private keys will be generated for communication data.

5.2.5. Encrypt Data in Motion

When a user is trying to access information from the hospital, SSL (Secured Socket Layer) or TLS (Transport Layer Security) can be used for securing data communication between the data server and the client. Connection starts with a TLS handshake (exchanging public keys) and before giving access to the data, several certificates are checked for authentication and security purposes. This was, SSL/TLS can avert man-in-the-middle attacks or data leaks.

5.2.6. Backup

The CAP team will accomplish the responsibility of scheduled backup of all the necessary data so that if data is lost from a server for any reason, then, there’s always backup data to avoid unavailability.

5.2.7. Update

CAP team will keep the system updated and patched for better safeguard and avoid security issues.

5.3. Testing and Audit

The privacy policies should force the hospital or organization authorities to follow proper logical and technical strategies to keep the security circle running with paramount importance given. To maintain privacy by protecting the data, a routine check-ups and governance chain has to be followed strictly. Healthcare organizations can ensure this stride by following the combination of testing and auditing strategy described below.

5.3.1. Testing

Testing will be done in the system development period. Ensuring privacy through proper use of the technologies is the main goal of testing. That might include the followings:

I. Checking that the system ensures strict authentication and authorization control as most of the attacks on systems are done primarily by getting access to associated accounts.

II. Secured coding by experts needs to be ensured during the development period of the system as inferior coding makes the system more vulnerable to the hackers. Ensuring the privacy of the users must be given highest priority while building the system. Design by strategy and design by default has to be implemented as per the security requirement of the system.

III. Penetration test or simulated cyberattack on the system must be done to identify vulnerabilities and system flaws before the system launch.

5.3.2. Audit

An audit team will do the continuous check-ups routine. The audit team must ensure the followings:

I. Risk assessment must be performed to analyze upcoming as well as existing risks. Risk assessment reports should be regularly generated and studied.

II. Collecting information regarding the network and access policies that includes LAN, WAN, Firewall etc. Log files generated from firewalls and local servers must be collected for analytical study. A full and complete list of password failures, lost password cases, lost credentials and outdated antivirus incidents must be kept. Vulnerability analysis must be done on all the information collected by the audit team to get updated about the magnitude of the existing cybersecurity flaws in the system.

III. The audit team should do a regular penetration test. They must generate test reports and fix the system if necessary.

IV. Another responsibility of the audit team would be to ensure proper knowledge on the user perspective. They will arrange a short training program for the employees on how they should act to protect the users privacy and maintain security in the healthcare organization. They can also send short training videos to employees and users for creating awareness about cybersecurity.

6. UNDERSTANDING THE THREAT AND PROPOSED SOLUTION MODEL

Threat modeling is an engineering solution that maps security flaws within the system with the system design and helps finding out the possible threats and vulnerabilities. We propose a separate threat model specialized for the healthcare sector. The proposed model consists of the following three steps.

6.1. Decomposition

In this step the system development team will hold several meetings with the healthcare organization authority and collect all the necessary information required to gain better understanding about the sophistication of data and security requirements. This step will enable the developer to map the user view with development perspective. They will try to find out the dependencies, the user domain of the system and the risk factors associated with each type of user.

6.2. Proposed Structure

In this step the development team will propose a system structure along with simple non-technical and understandable demonstration. The proposed diagram will show the data flow of the system along with the components that will be used. Our proposed system structure for healthcare organizations is attached below as shown in Figure 1.

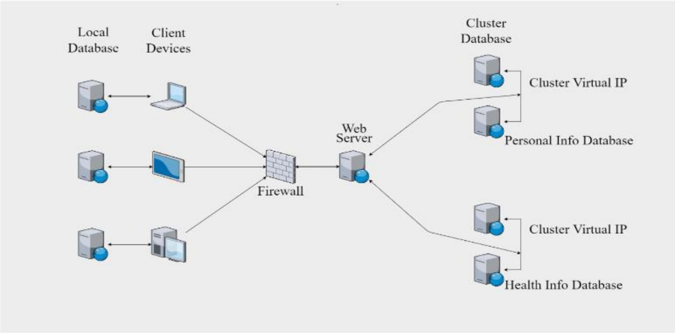

Figure 1: Proposed Data Storage and Data Flow Diagram.

We propose clustering of the database to ensure stable availability of data and to separate personal-healthcare data from regular data. Clustering means using more than one server that serves as a single unit. Clustering will also enable the system for load balancing and parallel processing.

6.3. Modeling the Threat Structure

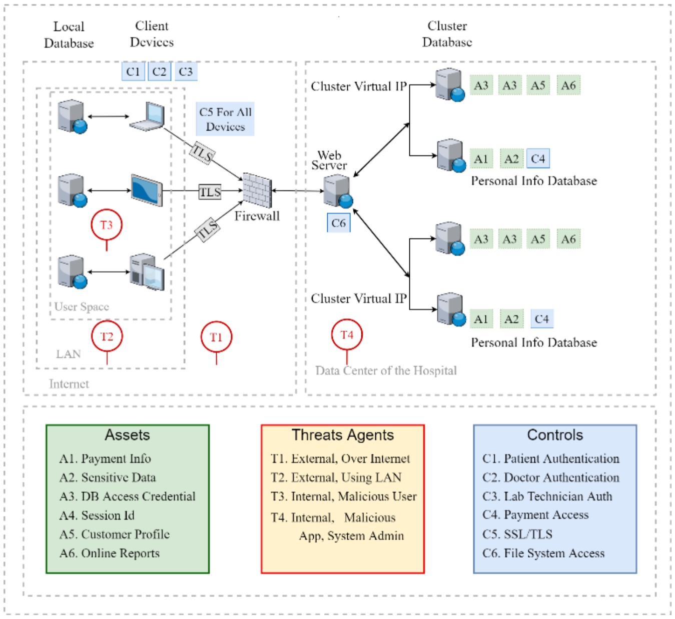

Figure 2: Proposed Threat Model

In this step, threats will be mapped to the system architecture design based on all the information collected from the authority. The threat modeling expert will find out the assets, security controls and threat agents and they will also find out the possible locations for each of them. The application of threat modeling with our proposed system structure is shown in the Figure 2.

All the possible assets, threat agents and controls are shown in the figure. The threat model also shows the location of each of them inside the system architecture. The assets are the data that needs to be protected with highest security. The security controls are the mechanisms that must be implemented to ensure reliability. Threat agents are external and internal actors who might propose threat to the system after deployment. As we can see from the figure, assets are primarily located in the database and data like payment information, database access credentials, session id, patient profile etc. Assets are marked with light green markers in the diagram. Controls are located both in the user side and server side of the system. On the user side possible controls are the credential authentication of the users and ensuring the use of TLS/SSL that ensures secure communication over the internet. Controls are marked with light blue markers in the diagram. Threats are of many types and they can be initiated from both external and internal environments. The possible threat initialization points are marked with red markers in the diagram. With the help of these threat models, healthcare organizations can optimize the network security and identify vulnerabilities while protecting the privacy of the users.

7. CONCLUSION

Bangladesh has taken all the steps to implement a fully electronic patient record system but there are no data security or protection laws in Bangladesh. Most of the private healthcare organizations in Bangladesh use electronic means of record keeping which is by all means necessary. But the data collection, storage or maintenance must ensure proper privacy, security and protection of these data as healthcare data is sensitive personal information.

In this work, we have proposed strategies for every step ranging from data collection to storage. This work also proposes a data flow diagram that hospitals and healthcare organizations should follow. On the other hand, despite taking proper measurements, some threats are always there either from inside the organization system or from outside. We have also included a proposed threat modeling to encounter the threats before they might appear.

8. FUTURE WORK

The proposed solution and strategies need to be tested and simulated to better understand the applicability, reliability and robustness of this model. Health data related to patients, hospitals, clinics that is data related to each and every healthcare related entity is needed. It has to be from the root level. In this paper, we have collected data from internet resources.

If more related data is available such as, about the number of village health centers, how many are active patients, how many hospitals (both private and public) are there from union to division level and their facilities; it will help better understand the scenario and design a proper threat model. Moreover, strategies depend on the client and stakeholders. For this reason, the current framework from the lowermost to uppermost level can be analyzed in future along with the proposed strategy and solution can be implemented on a smaller scale in real life. This will help to grasp the situation much better. After that a SWOT analysis can be done to define further works on this research.

REFERENCES

[1] K. Corbin, "How CIOs Can Prepare for Healthcare ‘Data Tsunami’," *CIO*, 14 Dec 2014. [Online]. Available: https://www.cio.com/article/2860072/how-cios-can-prepare-for-healthcare-data-tsunami.html. [Accessed 20 Jun 2020].

[2] "General Data Protection Regulation," *Intersoft Consulting*, [Online]. Available: https://gdpr-info.eu/. [Accessed 01 Jan 2020].

[3] “Personal Health Information Protection Act, 2004, SO 2004, c 3, Sch A”, [Online] Available: http://canlii.ca/t/549p5 [accessed: 05 may, 2020].

[4] 4.“Health Insurance Portability and Accountability Act of 1996 (HIPAA)”, [Online] Available: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html [Accessed: 02 May, 2020].

[5] "The total number of Mobile Phone subscribers has reached 165.615 Million at the end of January, 2020," BTRC, 12 Feb 2020. [Online]. Available: http://www.btrc.gov.bd/content/mobile-phone-subscribers-bangladesh-january-2020. [Accessed 14 Jun 2020].

[6] "The total number of Internet Subscribers February, 2020," BTRC, 26 Feb 2020. [Online]. Available: http://btrc.gov.bd/content/internet-subscribers-bangladesh-february-2020. [Accessed 13 Jun 2020].

[7] “Report on Bangladesh Sample Vital Statistics 2018”, Bangladesh Bauru of Statistics [Online] Available: http://www.bbs.gov.bd/site/page/b588b454-0f88-4679-bf20-90e06dc1d10b/- [Access: 11 May, 2020].

[8] “Annual Report HSD 2018-2019” Ministry of Health and Family Welfare Bangladesh, [Online] Available: http://www.mohfw.gov.bd/index.php?option=com_content&view=article&id=581&Itemid=190&lang=en [Access: 12 May, 2020].

[9] Realtime Health Information Dashboard, Directorate General of Health Service Bangladesh.[Online] Available: http://103.247.238.81/webportal/pages/index.php [Access: 12 May, 2020].

[10] K. Adane, M. Gizachew, and S. Kendie, “The role of medical data in efficient patient care delivery: a review,” Risk Management and Healthcare Policy, vol. Volume 12, pp. 67–73, 2019.

[11] K. Abouelmehdi, A. Benni-Hssane, H. Khaloufi. M. Saadi, "Big data security and privacy in healthcare : A review," *The 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks*, vol. 113, pp. 73-80, 2017.

[12] "Indiana Health Information Exchange," [Online]. Available: https://www.ihie.org/. [Accessed 01 May 2020].

[13] "Health Information at Risk: Successful Strategies for Healthcare," Intel, 2011. [Online]. Available: https://www.ehealthnews.eu/images/stories/pdf/successful_strategies_for_healthcare_security_privacy.pdf. [Accessed 29 April 2020].

[14] "Healthcare Data Breaches Costs Industry $4 Billion by Year's End, 2020 Will Be Worse Reports New Black Book Survey," CISION, 04 November 2019. [Online]. Available: https://www.prnewswire.com/news-releases/healthcare-data-breaches-costs-industry-4-billion-by-years-end-2020-will-be-worse-reports-new-black-book-survey-300950388.html. [Accessed 10 May 2020].

[15] "Cost of a Data Breach Report," IBM Security, [Online]. Available: https://databreachcalculator.mybluemix.net/. [Accessed 07 May 2020].

[16] M. Colesky, J. Hoepman and C. Hillen, "A Critical Analysis of Privacy Design Strategies," 2016 IEEE Security and Privacy Workshops (SPW), San Jose, CA, 2016, pp. 33-40, doi: 10.1109/SPW.2016.23.

[17] “Privacy Act 1988”, Australia [Online] Available: https://www.oaic.gov.au/privacy/the-privacy-act/ [Accessed: 06 may 2020]

[18] “Personally-Controlled Electronic Health Records Act 2012”, Australia [Online] Available: https://www.legislation.gov.au/Details/C2012A00063 [Accessed: 05 May, 2020]

[19] “Health Information Technology for Economic and Clinical Health (HITEC)”, 2009, USA, [Online] Available: https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html [Accessed: 07 May, 2020].

[20] “Health Information Privacy Code, 1994”, New Zealand, [Online] Available: https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/health-information-privacy-code-1994/ [Accessed: 08 May, 2020].

[21] “Patient Data Act, (2008:355)”, Sweden, [Online] Available: https://www.global-regulation.com/translation/sweden/2988365/patient-data-law-%25282008%253a355%2529.html [Accessed: 04 May, 2020]

[22] “Health Data Law, Federal Law No 2 of 2019”, UAE, [Online] Available: https://www.pwc.com/m1/en/publications/healthcare-data-protection-in-the-uae.html [Accessed: 08 May, 2020].

[23] “Data Protection Act, 2018”, UK, [Online] Available: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted [Accessed: 03 May, 2020].

[24] “Act on the Protection of Personal Information, 2017”, Japan, [Online] Available: https://www.ppc.go.jp/en/legal/ [Accessed: 02 May, 2020].

Authors

AKM Bahalul Haque is a faculty member at North South University. He has interest in research areas of IoT, Blockchain, Information Security, Artificial Intelligence. He achieved his B.Sc from Bangladesh and completed his M.Sc. from Germany. There are quite a few number of conference proceedings and journal publications are in his profile.

Tahmid Hasan is a research enthusiast. He is currently pursuing his undergrad in computer science and engineering from North South University, Dhaka, Bangladesh. He has a keen interest in academic career and research. His research interest includes machine learning, data security, computer vision and image processing.