Need and Importance of Healthcare Data Integrity

Alka Agrawal*[1], Nawaf Rasheed Alharbe[2]
[1]Department of Information Technology, BBA University, Lucknow, UP, India
alka_csjmu@yahoo.co.in
[b]Department of Computer Science and Information, Community College, Badr, Taibah University, KSA
nrharbe@taibahu.edu.sa

Abstract—**Recent security breaches have exhibited that the peril is no longer hypothetical, and industries ranging from healthcare, aviation and retail have all proved to be vulnerable. The attackers have now graduated from isolated incursions to the potential of launching a devastating strike on every sector. Cyber security shall not be considered as a state of perfection to be achieved and maintained. It is an ongoing process of self-evaluation and informed actions, adapting to the threat landscape as it evolves. Cyber operations that will manipulate data will be the next weapon for Cyber Armageddon in near future. The discussion focuses on the development of the breach of data integrity, an issue that has arisen in the wake of arguments against the recent trends of cyber-attacks. The breach of data integrity poses an arguably more unknown threat for healthcare industry to combat than simple data theft, as it can allow attackers to alter anything in the record. By nature, healthcare data integrity breaches are often difficult to detect and in many cases, where this type of compromises has occurred, the real impacts are yet to be diagnosed. The article explains some of the key benefits to be derived from maintaining data integrity, as well as the risks associated with the software industries in general and healthcare industries in particular if it is not observed strictly.**

Keyword - Healthcare Data; Data Integrity; Data Security; Cyber Security; Cyber Attacks.

I. INTRODUCTION

Data is the currency of the digital world and has become lifeblood of contemporary businesses. It has become a crucially valuable resource that dictates everything from business operations to government policy [1]. Hackers may run malicious code on the hacked systems and manipulate data. This is the emerging threat that has industry leaders scrambling and requires new thinking from security perspectives. In data breach, intruders break into a system and breach susceptible information. Data integrity exploitation will now be more dangerous in many cases. Software industries are routinely making data-driven business decisions. Those decisions can have major impact on company's bottom line goals, if data integrity is breached. Calculated and intentional manipulation to data can methodologically guide the opinion-making processes of those who use that data [2]. The motive behind data integrity attack is yet terrifying wherein attackers modify the data instead of stealing the information. Data owners may or may not be aware of these manipulations. By altering ground truths of any industry, data tampering has the potential to destroy prominence, both personally and professionally. Data Integrity attacks are not just about companies losing profits and customers [3]. Rather, it allows intruders to regularly intertwine with cyber security and public health and safety.

Undoubtedly, data has turned into one of the most valuable assets of any company. The more appropriate data an organization has, the more successful it is likely to become. This is where data integrity becomes key. Data integrity has become a serious issue over the past recent years and therefore is a core focus of many industries. Integrity ensures that the data is original, correct and safeguarded from unauthorized modification. Data integrity protection is security requirement. Untrusted data is devoid of integrity [4]. Data integrity is the essential aspect of any industry's security posture.

II. TRIGGERS OF DATA INTEGRITY LOSS

Ensuring licit access to privileged information has become an urgent concern. Due to the constant evolution of technology and the emergence of new practices and behaviors which they are enabling in cyberspace, new trends of cybercrime is coming up and cyber attackers are getting smarter and more sophisticated. US intelligence officials and security firms have identified data sabotage as one of cybercrime's next big fronts. Cybercriminals, state-patron intruders, and malicious agents use advanced techniques that amalgam multiple tactics including spear phishing emails and malware to penetrate organizations, steal sensitive data, and manipulate the same. Attackers are adapting another means to damage the reputations of individuals and companies by stealing and manipulate data.

Recent years have seen a plethora of data alteration attacks. Some of the major ones are illustrated here [5-7]. In 2015, attackers manipulated the number of recommended dose with Johnson & Johnson insulin pumps [8]. In 2016, Russian intruders compromised the systems of the World Anti-Doping Agency and released manipulated healthcare records of many famous athletes [9]. In 2017, research scholars at University of Tulsa managed to get the access to a wind farm's control system and installed application that would transmit false signals to the system [10]. In early 2018, President of the World Economic Forum declared that worldwide damage from cyberattacks reached USD 1 Trillion [11].

The cyber criminals are continuing to sharpen their focus on healthcare. The exploitable electronic information in health record brings a high price on the black market. Protecting data integrity breach in the healthcare industry is no easy feat. Ponemon Institute published a research on data breach in healthcare industry and reveals that the cyber-criminal attacks have increased by 125% since 2010 [15].

III. Areas Affected

Data integrity is the new buzzword in healthcare industry today. Since 2013, there has been a hilly rise in the number of data integrity breaches [14]. Data integrity-related issues have been uncovered around the world, and are expected to be high in coming years. Cybersecurity and data privacy are inextricably linked. Naturally, data confidentiality and privacy can only be achieved with effective security. Relentless swarm of successful cyber-attacks by means of manipulating data badly disrupts every area and requires enormous expenditures to patch the damage. Cyber criminals might even manipulate data in backup storage to ensure that there is no recovery.

Aviation: Cyber threats issue is identified as a new risk for aviation security [12]. Aviation is highly vulnerable as for as cyber terrorism is concerned. Cyber attackers may target airports and commercial airliners by penetrating the system and manipulating the data therein.

Healthcare: Healthcare industry is largely victimized industry in which attackers meddling of operations not only costs money, but also threatens lives. Healthcare is the area where cyber criminals may compromise data integrity to incur more human casualties in the near future.

Financial Industries: Bank has always been an object for nation-state launched hazard [13]. Banking institutions cannot afford to ignore the peril of third-party data breaches. Data security strategies in banks need protection against both internal and external threats.

IV. Data Integrity Breech in Healthcare Institutions

Preventing access to accurate data immediately triggers life-and-death consequences for patients under care. As a result of data integrity breach in any hospital, a patient could be given a life-threatening prescription or the wrong procedure, leading to significant legal liability. Manipulated data is often walking right through the front door of health institutions in the hands of cybercriminals. According to the Federal Trade Commission, 19 people become victims of identity theft every minute [16]. Stultifying healthcare industry is comparatively easier than in other industries because of systematic underinvestment in cyber security within the healthcare industry. Further, medical devices that continue to run with vulnerable operating systems are also difficult-to-update. In a study, a massive 94% of health care industries reported having been victims of cyberattacks [15].

V. Attackers Evolutionary Approach- CIA or ACI?

Cyber Security requires a collaborative approach driven from the boardroom down and includes people within the institution. The traditional security triad is *Confidentiality*(C), *Integrity* (I), and *Availability* (A). As most security experts recognize the security prioritization for CIA in that order and guarantee Confidentiality, Integrity and Availability in that order. Attacks that transform from a breach in confidentiality to exploit integrity reaching to reduce availability are seen as being a good trade-off. Worry about cyber threats to critical public infrastructure is growing as these threats increase in both sophistication and prevalence. Threat sophistry has significantly changed; goal of the attackers, attack vectors and propagation methods of the attacker have evolved. There is a gradual evolution of cyber threats and breaches and their ill intension and objectives. Figure 1 shows evolutionary epochs of threats to data in the domain of cyber security.

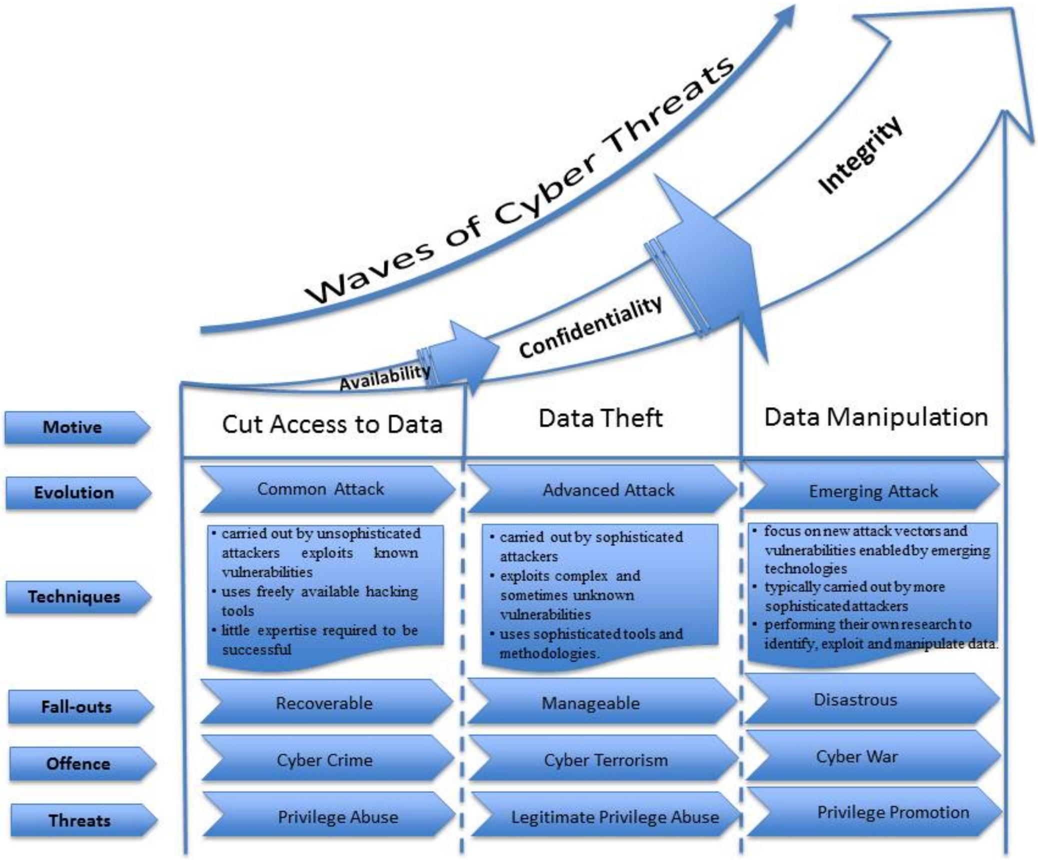

Fig. 1: Cyber Threats Waves

In contrast, initially attackers came with Common Attack to breach data Availability by cutting down the access to the data. Naive intruders with little expertise carried out this by manipulating known vulnerabilities using available tools and techniques. Generally, the intension of breach was to deny the access of the object under attack. Data under this attack was found to be Recoverable. Then, more advanced sophisticated attackers came and adopted Data Theft approach with Advanced Attack to exploit complex and sometimes unknown vulnerabilities using sophisticated tools and techniques. Their basic goal was to earn money. Now, recently, an Emerging Attacks to Manipulate Data has been noticed with a new attack vectors and vulnerabilities enabled by emerging technologies. This kind of the attack is typically carried out by more refined attackers performing their own expertise to identify, exploit and manipulate vulnerabilities.

VI. DATA INTEGRITY DIMENSIONS

There are three dimensions to data integrity that are shown in figure 2 and described as follows:

Secure Communication: Secure communication ensures communication security over public and local networks. Data passed in such a way as to keep them secret from anybody except the intended receiver.

Safe Storage: Storing data safe involves preventing unauthorized access of data as well as preventing accidental or intentional destruction, infection or corruption of information. Safe data repository is necessary for industry dealing with sensitive data to avoid data manipulation and to ensure uninterrupted operations.

Planned Audit: Data auditing has become very essential for the organization that works with sensitive data. At every stage where changes are made, bugs are allowed, modifications and alterations are detected, and data shall be audited and verified.

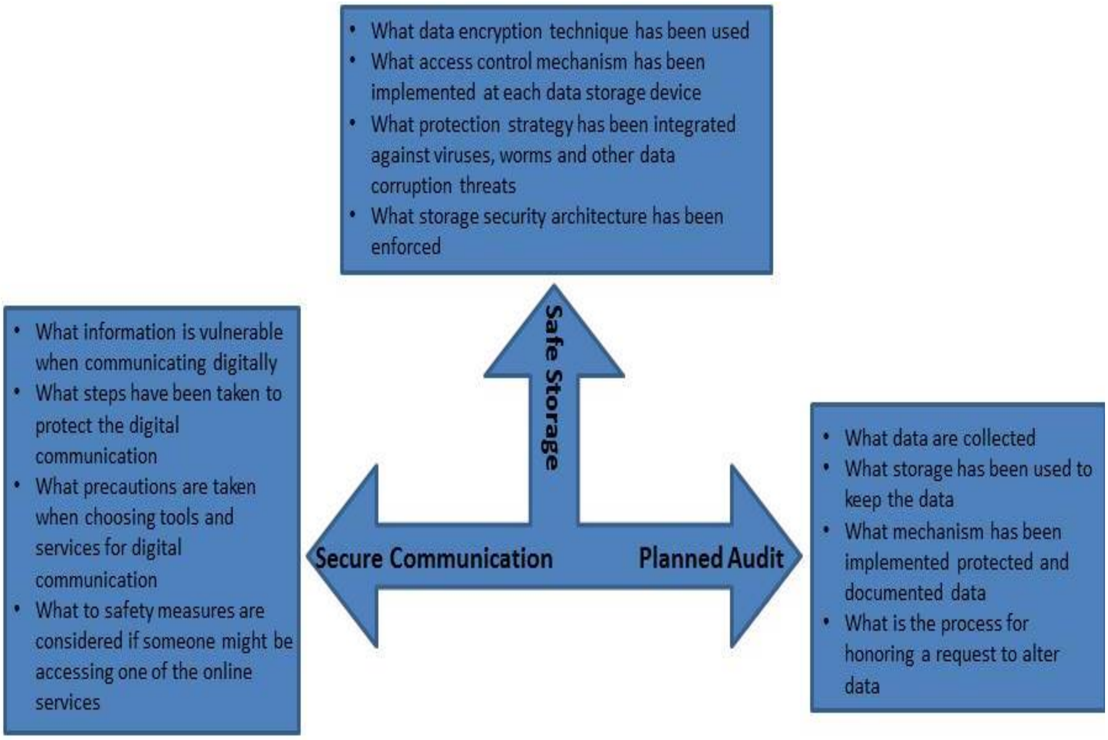

Fig. 2: Dimensions of Data Integrity

VII. Strategy to Minimize Data Integrity Breach

A defense mechanism against security threats in the form of data monitoring systems has become an urgent need to fight with data integrity breach. An effective means are required for specifying, detecting, and responding to anomalous behavior of data and data accesses caused by users and applications. By integrating data monitoring technology alongwith identity management, data security can be enriched. This will give deeper insight into the 'what, who, when and where' of data access and manipulation. In order to protect data integrity breach, organizations have to grow their base of security intelligence and efforts should be made to provide the right data to the right stakeholder. Figure 3 depicts the recommended a general walkthrough to minimize data integrity breach.

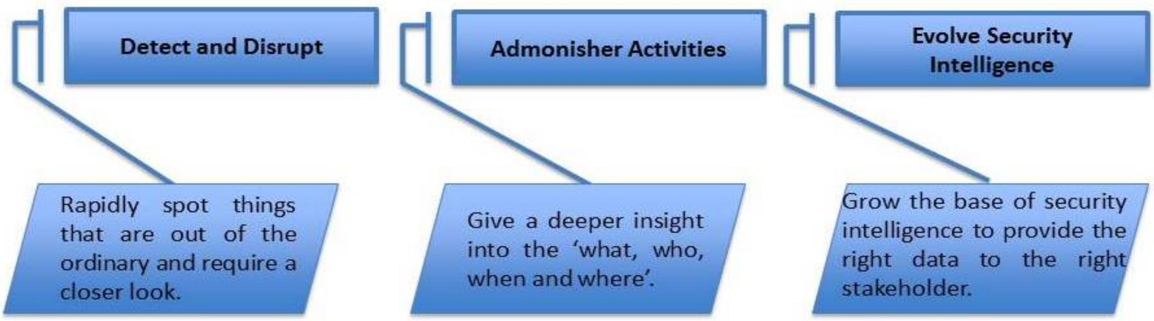

Fig. 3: Strategy

VIII. Integrity Monitoring and Control

We are breathing in an age of data. Data is critical in any sphere of organization and is any company's biggest asset. Contemporary systems are data dependent since the data is devoured and engendered at miraculous levels, periodically exchanged between many processes, individuals and systems. It is not enough to have data, however, as one must also have data integrity. Since big data analytics increasingly drives decision-making, integrity of data has become a considerable threat for researchers and security experts. Data integrity compliance and thereby trustworthy, complete and accurate data are mandatory for assuring the quality, safety and efficacy of system. Attaining data integrity is not so easy. There are various stumbling blocks in the way. In order to assure data integrity, there is an urgent need to establish strong integrity monitoring and control module as shown in figure 4, which shall help shield and cultivate data during processing, collection and storage.

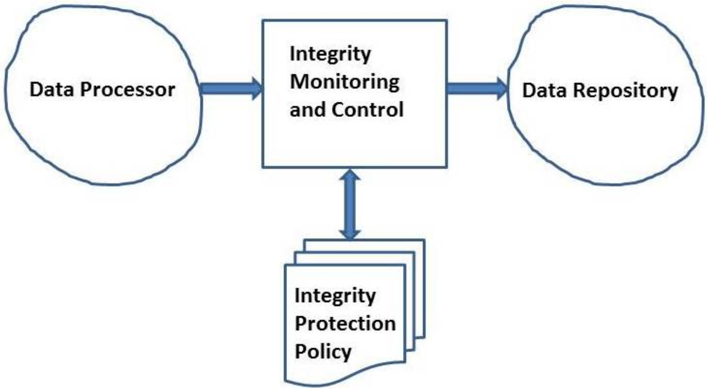

Fig. 4: Monitoring and Control Module

Integrity monitoring and controls module should be an integral part of system, helping to enforce an organization's data integrity goals. This monitoring module will be used to prevent semantic user errors, to protect against unauthorized data manipulation, to help prevent exploitation of vulnerabilities, and to stop malicious code from accessing the system. Integrity monitoring and control module will apply integrity protection policy that verifies the data operations, ensuring that data is not altered by applying integrity control features. General objective of Date Integrity Monitoring and Controls Module includes the following:

- To develop and implement policies indicating when the alteration of data is permitted.
- To protect data against intrusion, corruption, damage, modification, or destruction by implementing access controls
- To carryout auditing and quality monitoring for assuring data safeguard.

IX. CONCLUSION

There is no way to be staying safe from attack. An extended approach to cyber security accepts that ongoing cyber threats are an unavoidable part of doing business. Cyber security has become the primary priority across the globe as this faceless threat intensifies. Organizations have gotten pretty good at availability and are getting better at confidentiality. Unfortunately, they tend to think that built in integrity auditing is tickling integrity. Attacks aimed at altering with data integrity are reason for concern. Consequence of stolen data is obvious. But what if data is breached, but rather altered? With new threats reported every day it seems that the war on cybercrime is an uphill battle that cannot be easily won. However, healthcare industry can develop overall understanding of the risks posed in order to achieve much more secure position. None of the technology can completely ensure the system's impenetrability. But, implementing appropriate suggestive measure can make the industry less of a target resulting the best position to thwart attacks that may be attempted. It becomes obvious that the most likely weapon of the cyber terrorist is the breach of data integrity. Organization shall establish a means to address pertinent challenges in preserving data integrity. The healthcare data shall be safeguarded from malevolent altering, thus providing an assurance for data reliability.

REFERENCES

[1] W. Nikolaus Probst, How emerging data technologies can increase trust and transparency in fisheries, ICES Journal of Marine Science, Oxford University Press, (2019).

[2] P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp,S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, Spectre Attacks: Exploiting Speculative Execution, ArXiv e-prints, (2018).

[3] Hahn, A. Ashok, S. Sridhar, M. Govindarasu, "Cyber-physical security testbeds: Architecture application and evaluation for smart grid", IEEE Trans. Smart Grid, 4(4), (2013), 847-855.

[4] D. Linden, A. Rashid, The Effect of Software Warranties on Cybersecurity, ACM SIGSOFT Software Engineering Notes, 43(4), (2018), 31-35.

[5] Z. Zieliski, J. Chudzikiewicz, J. Furtak, An Approach to Integrating Security and Fault Tolerance Mechanisms into the Military IoT,In: Chakraborty R., Mathew J., Vasilakos A. (eds) Security and Fault Tolerance in Internet of Things. Internet of Things (Technology, Communications and Computing). (2019), Springer.

[6] Data Integrity Attacks: Is Data Manipulation More Dangerous than Theft?, Zettaset. 13 February 2018. Accessed February 2019. https://www.zettaset.com/blog/data-integrity-attacks-data-manipulation-more-dangerous/.

[7] Somayaji, M. Locasto, J. Feyereisl, The Future of Biologically-Inspired Security: Is There Anything Left to Learn?, Proceedings of the 2007 Workshop on New Security Paradigms, ACM, (2007), 49-54.

[8] J&J Warns Diabetic Patients: Insulin Pump Vulnerable to Hacking. Reuters. 4 October 2016. Accessed March 2019. https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e/jj-warns-diabetic-patients-insulin-pump-vulnerable-to-hacking-idUSKCN12411L.

[9] Russian Hackers Breached Athletes' Data, World Anti-Doping Agency Says. National Public Radio. 13 September 2016. Accessed March 2019. https://www.npr.org/sections/thetwo-way/2016/09/13/493776953/russian-hackers-breached-athletes-data-world-anti-doping-agency-says.

[10] How an Immune-System Model Mitigates Risks from Cyber Attacks on the Power Grid. WindPower-Engineering & Development. 18 December 2018. Accessed March 2019. https://www.windpowerengineering.com/connectivity/cybersecurity/how-an-immune-system-model-mitigates-risks-from-cyber-attacks-on-the-power-grid/.
[11] How Hackers Rob Banks. Positive Technologies. 21 May 2018. Accessed March 2019. https://www.ptsecurity.com/ww-en/analytics/banks-attacks-2018/.
[12] H. Assal, S. Chiasson, Think Secure From The Beginning, A Survey with Software Developers, ACM, (2019), 1-13.
[13] T. D. Oyetoyan, M. G. Jaatun, D. S. Cruzes, Measuring Developers' Software Security Skills, Usage, and Training Needs, Exploring Security in Software Architecture and Design, Vol 1, (2019).
[14] K. Ball, S. D. Esposti, S. Dibb, V. Pavone, E. Santiago-Gomez, Institutional Trustworthiness and National Security Governance: Evidence from Six European Countries, Governance, 32, (2019), 103-121.
[15] Filkins B. SANS health care cyberthreat report: widespread compromises detected, compliance nightmare on horizon. Norse. February 2014.
[16] Data breach at major healthcare firms, Computer Fraud & Security, Volume 2019, Issue 6, June 2019, Pages 3, 19.