INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact Factor: 6.078

(Volume 10, Issue 1 - V10I1-1281)

Available online at: https://www.ijariit.com

Understand the escalating trends of cyber frauds in India: a special focus on health care centers

Hrithik Kumar
hrithik.kumar@s.amity.edu
Amity University, Nijampur Malhaur, Uttar Pradesh

Dr. Hitesh Keserwani
hkesarwani@lko.amity.edu
Amity University, Nijampur Malhaur, Uttar Pradesh

Cybersecurity poses a threat and security of various security centers including health care. there are various digitization services in India, that led to growing certain trends of cyberfraud in target healthcare centres. this literature survey aims to present evidence to cyber fraud with special reference to health care centers. I review certain reports and articles to get an idea about various research papers. the survey aims to identify common types of cyber fraud that target health care centers, and vulnerabilities, impact on patients and healthcare providers, and apply various strategies of prevention. the survey involves enhancing awareness and cyber fraud trends in healthcare centers. inform policy decisions and guide cybersecurity measures.

Important keys*: health care centres, cyber fraud, vulnerabilities, strategies*

I. INTODUCTION

BACKGROUND

India's healthcare centre is growing at a faster rate. Including digital technologies and extra care of patients and management of the health care centre. The country has reported growth in internet as well as smartphone usage led to increasing online activities, and transactions related to health. Digital transformation is required in health care services. there is an increase in medical data, no of patients as well as health care centres.

HISTORY DATA

It led to the evolution of cyberfraud's in India and other countries as well. as their types, methods, and impact in healthcare centres. It gives a track of incidents such as cyber-attacks, phishing, identity theft, and other fraud activities targeting healthcare institutions. Analysis of historical data in understanding the patterns and cyber criminals in health care centers.

DEFINITION

CYBER FRAUD: criminal activity conducted by computer systems on the internet, to cause harm and to get financial gain

HEALTH CARE CENTRES: facilities provide medical facilities – hospitals, clinic, health care organizations.

TRENDS: tendency indicates direction, and nature of the development in health care centre concerning increase cyber frauds in India.
OTHER TRENDS – refer to rising trend and indicating the impact in cyber frauds in healthcare
Refer to different trends and the impact of health care, impact of health care, cyber frauds.

IMPORTANT

RAMSOME WARE ATTACKS – Malicious software that demands payment for the release and they are used to take out money from financial institutions by disrupting some services.

PHISHING – An attempt to obtain sensitive information that is username as well as password, credit card information, and electronic information also.

BREACHING OF DATA – wrong access of data, taking out of confidential information that as medical records, data of a patient, or financial data, they harm individual persons.

IDENTITY – the use of a person confidential information such as financial information. This information are used to commit other crimes. some fraud persons give medical services by using false methods.

HEALTH INFORMATION LAWS – regulations that give protection to medical records and health data, such as (HIPAA) in us and personal data in India.

II. MATERIALS AND METHODS

LIST OF MATERIALS USED IN EXPERIMENTS

the materials used in experiments are especially for actual research topic that give access to actual research papers. Our system get a basic list of instruments and raw material that we use to understand certain trends of cyberfraud in healthcare centers. we keep in mind some specific elements such as the objective to do so as well as the methodology.

COMPUTER – a collection of data, analysis of data, and simulation of cyber frauds.
INTERNET – some fraud occurs online, the internet is important to collect data, and online interviews as well as surveys are necessary.
SOFT WARE TOOLS – some software tools can be used for analysis of data and visualization of the data. for example – statistical analysis software. cyber security tools.
DATA SETS – cyber fraud incident data, attempts, attacks, some infections. they are essential to understand trends as well as patterns in some centers.
QUESTIONAIRE – to gather knowledge from
professionals such as teachers, workers, victims, and other experienced persons. Experience of stakeholders.
GUIDES – certain methods like interview, that ensures the structure of data collection.
RESOURCES – certain reports, article, and some resources as well that are related to cyberfraud's as well. they are collected to give support to certain findings.
SECURITY DEVICES – sub keys, certain tools, certain mechanisms that protect sensitive data. they save the data from the access of others.
MEASURES OF PROTECTION – privacy to data, protocols, data storage, certain techniques, safe sensitive information that is collected in particular research.
CONSULTATION – management in health care and analysis of data. to increase the quality of research.
TRAINING – educate the people who participate and raise the awareness of others about certain risks related to cyber fraud in health care.
BUDGET – resources to be required to do research. expenses due to the collection of data, licenses, fees related to publication.

STEP – BY – STEP PROCEDURE

- Literature review
- Identify key stakeholders.
- Data collection
- Analysis of certain trends of cyberfraud's.
- Assessment of certain risks.
- Compliance of certain regulations.

- Training
- Certain strategies of mitigation.
- Continuous evaluation
- Collaboration as well as knowledge sharing.

RESULTS AND DISCUSSION
DATA – VISUALS, GRAPHS, ETC.
RESULT ■ EXPLANATION OF DATA

- **COLLECTION OF DATA**
  Reports of government agencies and cybersecurity firms institutions and certain publications. Data related to cyberfraud's. types of cyberfraud's and their frequency, affected regions related to it. impact on software and society as well.
- **DATA ANALYSIS**
  The collected data is analysed by certain trends and patterns of some healthcare centres in our country. The categorization of data based on nature, target and methods of use.
- **VISUAL REPRESENTATION**
  The data is gathered and analysed in India. the visual representation in the form of certain graphs as well as charts and present your data as findings with it.
- **INTERPRETATION OF DATA**
  Provide insights for visual representations. significance of trends and potential implications on health care centres in India. Discuss some reasons the trends of cyberfraud's and purpose recommendations for some challenges in our country.

TOOLS & INSTRUMENTS USED FOR DATA ANALYSIS
ENSURE RELIABILITY OF EXPERIMENT

Here certain tools and instruments that are commonly used are

- SOFTWARE FOR STATISTICAL DATA • VISUALISATION DATA TOOLS
- MINING OF TEXT AND NLP.
- NETWORK ANALYSIS
- DATA MINING SOFTWARE.
- QUALITATIVE DATA ANALYSIS SOFTWARE.
- CLEANING OF DATA
- PLATFORMS OF COLLABORATION.

SOFTWARE FOR STATISTICAL DATA • VISUALISATION DATA TOOLS

The year 2011 closed out with another privacy-oriented brouhaha, this time surrounding Carrier IQ, which sells analytics software for mobile devices. The software is used in an estimated 142 million smartphones. A systems analyst/amateur security researcher discovered this software on his smartphone and found that it was capturing battery life, connections, text messages, emails and other actions. A slew of accusations followed, with Carrier IQ and its carrier customers being taken to task for allegedly keylogging, spying and tracking. But a more detailed analysis by other professional security researchers found that the systems analyst who originally raised the issue was confusing Carrier IQ's actions with those of debug statements mistakenly left in the Android code by phone maker HTC's programmers. As it turns out, Carrier IQ was simply collecting performance data for optimizing the end users' experience. Nevertheless, the original discovery prompted Sprint and HTC to reportedly no longer include the Carrier IQ software on their devices.

MINING OF TEXT AND NLP

No company is more aware of the danger posed by poor third-party code than Yahoo, which has suffered several high-profile incidents in recent years. In 2010, Yahoo acquired the online publishing platform Associated Content and rebranded it as Yahoo Voices. Even though the rebranding process didn't take long, Yahoo didn't immediately integrate the Yahoo Voices accounts into its authentication process; rather, it relied on its existing platform. Two years later, a hacker found a SQL injection (SQLi) vulnerability and used it to penetrate the Yahoo Voices servers, collecting more than 400,000 usernames and passwords. A similar attack occurred later that year when a hacker used SQLi to gain access to AstroYogi, an India-based astrological website. The problem for Yahoo was that it contracted with AstroYogi and rerouted users from its Lifestyle site to the affected astrological website, which operated under the Yahoo brand. Because user credentials had to be sent to the vendor, the hacker had access to the credentials of any user visiting the astrology site. In this particular case, the hacker appeared to be benign (going public with the hack only after Yahoo ignored requests to fix the vulnerability), but Yahoo's reputation certainly took a hit.

NETWORK ANALYSIS

A recent case of Snapchat who finally let users knows that third-party apps are saving their pictures and videos. A third-party website named SnapSaved.com allowed users to covertly save incoming messages by giving their login details to the site. This let Snap Saved access Snapchat's servers on their behalf and store their images permanently on the site, which was itself hacked by unknown individuals. Snap Saved was a website (it's now offline) while Snap Save is an app. The two programs offered an identical service and used similar branding but appear to be unconnected, with the creator of Snap Save (that's the app) telling tech site Engaged: "Our app had nothing to do with it and we've never logged usernames/passwords."

DATA MINING SOFTWARE.

There are some data mining software are :

Rapid miner: it is a user-friendly interface. it also offers data mining as well as machine learning tools.

Weka: it is an open source software that has machine learning software and data mining tasks.

SAS enterprise miner: it gives comprehensive solutions to data mining and predictive modeling. It offers a wide range of algorithms as well as analytics capabilities.

IBM SPSS Modeler: it is a data miner and text analysis software and do model deployment.

Microsoft SQL Server Analysis Services: it gives mining functionality for patterns and trends in India.

There are examples and choices of some software that depend on factors that specify the requirements of our project, my budget, and familiarity with certain tools.

QUALITATIVE DATA ANALYSIS SOFTWARE.

The researcher organize, decodes as well as analyses data such as texts, image, and QDA miners.

Software that offers certain features that is coding and decoding categorize and visualised. that do needs of research and other preferences.

CLEANING OF DATA

That is to detect and correct errors as well as inaccuracy of some sets of data. They improve the quality of some data.

1, remove data
2. To delete and manipulate of data.
3. Some data values as well as formats.
4. data transformation
5. correcting some formats.
6. correct words and meanings.
7. correct missing words.
8. make some presentation.
9. make guidelines for some data.
10. correct some silly mistakes.

Cleaning of data leads to accurate and good information that is useful to do some work.

PLATFORMS OF COLLABORATION

The platform is doing some communication as well as teamwork. The platform is across various locations including:

1. Teams – it includes chatting and making videos. Storage of file. Applications for various collaborations.
2. Slack – that always offers some channel to it. File sharing as well as integration.
3. Zoom – it is used for online conversations with people. Use whiteboard online. Sharing of the screen of all laptops.
4. Asana – it organizes track work , it assignment of tasks. It led to tracking the progress of reports.
5. Share point of Microsoft: it refers to the management of some documents, and organizational features As well as to collaborate with the security of content.
6. G suite of Google – it provides Google Drive, google docs, as well as Google Meet to their customers.
7. Camped of base – it provides messaging, file sharing as well as scheduling to meet the demand of their customers.

8. Jira – it provides issues for tracking management of project, and tools development.
   These tools help with the communication process, and integration of systems. It depends on the size of the team.

OBJECTIVE – WHAT YOU PLAN TO ACCOMPLISH

- IDENTIFY CERTAIN PATTERNS
- ACCESS TO CERTAIN VULNERABILITIES

- UNDERSTAND CERTAIN MOTIVES
- ANALYSIS OF CERTAIN IMPACT
- LEGAL FRAMEWORKS
- BEST PRACTICES STRATEGIES
- RECOMMENDATIONS OF CERTAIN POLICIES.

II. LITERATURE REVIEW

- The cyber security challenges in indian health care by r.gupta : trends and solutions . international journal of health care management.
- This paper is all about the cybersecurity challenges faced by various organizations. rising incidence of cyberattacks. to purpose strategies enhancing cybersecurity. mitigating risk in health care.
- It analyses the types of cyber security threats and vulnerabilities prevalent in health care centres. to take cybersecurity measures and approaches to address threats.
- The impact of cyberfraud's in patents and health care providers. find consequences of cyberattacks, and robust cybersecurity protocols.
- It gives recommendations for the Indian government to mitigate cybersecurity risks in healthcare sector.
- Regulate frameworks, cyber security standards,

RESEARCH GAP – WHAT HAS NOT BEEN SOLVED OR ACCOMPLISHED

Understand the trends of cyberfraud in India, a complex and multifaced research area . some research conducted on cyber security threads in some sectors, there are potential research gaps. unanswered questions.

- NO COMPREHENSIVE DATA
- CHALLENGES IN DATA SECURITY
- THREATS AND TACTIC.
- PATIENT CARE AND SAFETY.
- COMPLIANCE
- PUBLIC EDUCATION

- Existing studies rely on some evidence or limited data sets, made it challenging to have full scope and nature of cyber frauds in various countries.
- Health care data is sensitive, containing personal and medical care knowledge. that information is important to cyber criminals.
- Research deals with some challenges related to health care in safe the data.
- Cyber criminals are constantly working on their abilities and techniques.
- Some threats in country such as virus, new malware, and problems in healthcare it systems.
- Significant attention to threats in health care centres.

- Factors in insider threats and strategies to get employee awareness.
- Reduce risk of internal fraud.
- Financial risk that have an impact on safety of patients. to examine the certain consequences of cyber frauds on delivery such as healthcare services on our country.
- There are various guidelines for enhancing data protection and cybersecurity of data in health care as well in specific areas such
  as accounting and to make something portable. and protect bill for personal data.
- Effectiveness of certain regulations in cyberfrauds. explore challenges related to compliance.
- The level of cybersecurity- is crucial in prevention and responsive strategies. it involves cybersecurity practices, resources, healthcare organization capabilities & identifying areas of improvement.
- Lack of awareness about healthcare professionals, patients, the general public as well as the risk of cyberfraud's.
- Awareness campaigns and educational initiatives and plans to enhance public understanding of cybersecurity issues in health care.
- To address certain gaps that led to a comprehensive understanding of certain trends related to cyber frauds in Indian centres led to the development of targeted inventions to reduce risks.

III. DISCUSSION

■ ATTACHING MEANING TO RESULT IN THE PRESENT RESEARCH CONTEXT.
The research elucidates on certain cyber frauds in some healthcare centres in our country. they analyse the severity and frequency of incidents. by examining the no of cases in the report. care of certain patients.
certain methods and techniques targeted by cybercriminals. These should include ransomware, cyberattacks, breaching of data, and tactics of engineering. take preventive measures and cybersecurity strategies.

- VULNERABILITIES – that are susceptible to cyberfrauds. that is outdated software, and security training among staff members. certain measures for staff data. cybersecurity infrastructure.
- MOTIVATIONS – whether it's a financial gain, sensitive data of a patient, health care services, or motivation to inform strategies for prevention.
- PATIENT CARE AND TRUST AS WELL – consequences for financial loss, the confidentiality of patients, no health services, no trust in the health care system, to access the impact of cyber frauds on the quality of patients, trust of patients, and health outcomes. Regulations related to HIPAA is for safeguarding data of patients. to find out the no of compliance in health care centers against data breaches and cyber frauds as well. it can guide some makers of policy to increase regulations.
- PREVENTIVE MEASURES – to invest in some robust cybersecurity health centers. conduct risk assessments implement training programs and promote a culture of cybersecurity awareness.

IV. CONCLUSION

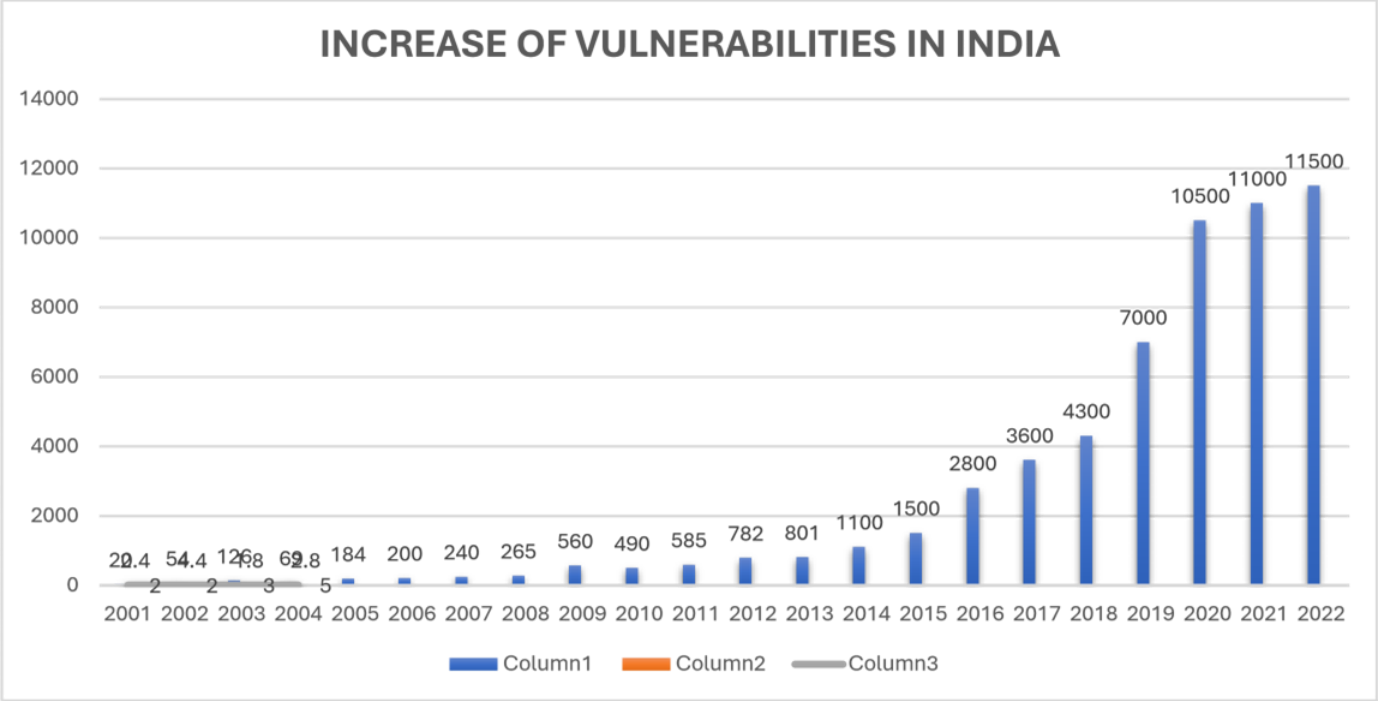
OBJECTIVE
EMERGE PATTERNS – the primary objective is to identify and understand the trends of cyber-attacks. analyze the patterns of cyber-attacks. target cyber-attacks.
QUANTIFY SCOPE—it involves collecting different amounts of data based on the frequency and severity of certain cyber incidents. it incurs certain cyber losses. it gives rise to an impact in the care of patients.
VULNERABILITIES – outdated technology, improper measures of cybersecurity, staff training, and compliance issues as well.
IMPACT – to understand the broader impacts, and consequences on patient quality care, health care trust, and compliance.
MITIGATION – cyber security measures to understand and address the in Indian health care centres. improve cybersecurity infrastructure, to improve staff training, and improve a culture of cybersecurity awareness.
POLICY AND PRACTISE – aims to inform policymakers, administrators, and professionals to the evolving nature of the cyber threat in healthcare centres. it shapes policies, practices, and investments to improve cyber security and protect the data of certain patients.

REVIEW KEY FINDINGS
INCREASE IN FREQUENCY – it indicates an increase in the frequency and severity of cyberfraud in our country. it suggests health organizations to become prime targets in case of cybercriminals.
TARGET METHODS – it includes phishing attacks , malware, tactics, vulnerabilities in it infrastructure, and human factors.

DATA BREACHES – it can compromise the confidentiality and integrity of certain information of patients. it gives rise to privacy and potential identity theft.
FINANCIAL – it led to direct financial losses that occurred from ransom payments as well as data recovery. it led to regulatory fines.
CARE OF PATIENTS – direct impact on quality of patient care. it services disruption, medical records lost. it rises to a loss of trust.
SHARING OF INFORMATION – in the rising of threats, the importance of collaboration and sharing of information with government agencies, industry stakeholders, and cyber security experts. to combat cyberfrauds. issue and ensure that if third-party software is required it is properly maintained and patched.

IMPLICATIONS OR APPLICATIONS

- enhances measures of cybersecurity
- staff training and programs of security.
- regulatory compliance.
- information sharing • cyber insurance investment.
- incident response.
- campaigns related to public awareness
- research & development.



IV. REFERENCES

[1] some databases like PubMed, Google Scholar, IEEE Xplore, and JSTOR. Searching using keywords such as "cyberfrauds in India healthcare," "healthcare cybercrime trends India," or "healthcare cybersecurity challenges." You may need to design your search terms based on the results you obtain.
[2] the Ministry of Electronics and Information Technology (MeitY), and the National Health Authority (NHA). These various sources may provide some insights into cybersecurity challenges specific to healthcare centers in India.
[3] Look for reports and whitepapers from some firms, cybersecurity companies in India, and the industry. Firms like PwC, Deloitte, KPMG, and EY often publish some research papers on cybersecurity trends and challenges in some sectors, including health of the patients.

