IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, April 2023
Impact Factor: 7.301

Data Security and Privacy Protection in Web in Indian Environment

Sajid Momin[1], Sachin Avghade[2], Sonali Chavan[3]
Faculty, Rajarambapu Institute of Technology, Islampur, Sangli, Maharashtra, India[1]
Faculty, Rajarambapu Institute of Technology, Islampur, Sangli, Maharashtra, India[2,3]
sajid.momin@ritindia.edu[1], sachin.avghade@ritindia.edu[2], sonali.chavan@ritindia.edu[3]

Abstract: *This paper deals with the privacy issue in Indian perspective with respect to challenges in three different dimensions like Legal, Technical and Political domain. We have research to deal with these challenges. Advancement in technology such as remote accessibility, Data interchange Mining, Cloud computing etc. brings unforeseen challenges and one of the major challenges is threat to "privacy and protection". There have been a plethora of developments in the privacy and data protection space in India. Data, off late, has been looked at by many very differently today in terms of value and treatment. There appears to be some rationale in the new saying that data is the new mark material [8].*

Keywords: Privatus, legislative framework, Segmentation, Privacy Act, e-court

I. INTRODUCTION

The word privacy has been derived from the Latin word "Privatus which mean separate from other. It can be define as capability of an single or group includes themselves or information about themselves and thereby reveal themselves selectively. Privacy can be understood as a right of an individual to decide who can access the information, when they can access the information, what information they can access [2] [4] .

A use of data for businesses today is vital for businesses to survive and lucrative if used efficiently. Data is the key for innovation, desirable customer experience and driver for competition. Without data, organizations would struggle to innovate or offer memorable experiences to consumers, both affecting technological developments and consumer choices and variety. To handle major cyber challenges we refer ITA Act 2008 that was built with the motivation to facilitate e-commerce and hence the privacy was not prior concern in IT act [3].

Indian constitution defines the privacy as personal liberty in Article 21. Article 21 states that "No person shall be deprived of his life or personal liberty except according to a procedure established by law." Thus, article 21 secures two rights:

- Right to life, and
- Right to personal liberty.

"Protection of Life and Personal Liberty" No person shall be deprived of his life or personal liberty except according to procedure established by law. The privacy is considered as one of the fundamental rights provided by constitution in list 1. Privacy is recognized at international level as Human Rights in different dimension as

- Privacy of person
- Privacy of personal behavior
- Privacy of personal communication
- Privacy of personal data.

The word privacy differs from the word confidentiality. We use words privacy, confidentiality and information security synonymously but these words have different meaning and different scope [3].

II. LEGAL CHALLENGES

In Indian context there is a lack of proper privacy legislation model so it is extremely difficult to ensure protection of privacy rights. But in absence of specific laws there are some few proxy laws or incident safeguard that the government is using for privacy purpose.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, April 2023
Impact Factor: 7.301

Certain legislative framework that provides indirect support to privacy concerns in India, like Article, Indian Constitution, IT Act 2000, and Indian Contract Act 1872 [1].

There is following bullets is present Indian legal frame work for privacy

- No comprehensive law and still the privacy issue is dealt with some proxy has no convergence on the privacy issue.
- No classification of Information as public information, private information sensitive information.
- No legal frame work that talks about ownership of private and sensitive information and data
- No certain procedure of creating, processing transmitting and storing the information.
- Lack of any guideline that defines about Data Quality, Proportionality and Data Transparency.
- No framework that deals with the issue of cross-country flow of information.

A list of technologies that have the potential to impact on privacy like Biometrics (such as fingerprints, hand geometry, face, voice, iris and keystroke recognition),Radio frequency identification (RFID),Smart cards, Voice over Internet Protocol (VoIP),Wireless technologies.

III. DATA ENCRYPTION PROCESS

Encryption in cyber security is the conversion of data from a readable format into an encoded format. Encrypted data can only be read or processed after it's been decrypted.

Encryption is the basic building block of data security. It is the simplest and most important way to ensure a computer system's information can't be stolen and read by someone who wants to use it for malicious purposes [7].

Data security encryption is widely used by individual users and large corporations to protect user information sent between a browser and a server. That information could include everything from payment data to personal information.

Data encryption software, also known as an encryption algorithm or cipher, is used to develop an encryption scheme that theoretically can only be broken with large amounts of computing power

IV. CLOUD SECURITY ARCHITECTURES

Cloud security architecture typically includes components and best practices relevant to the types of cloud security services the business wishes to secure. Examples include an AWS cloud security architecture, Google infrastructure security, or an Azure security architecture. Additional key components of cloud security architecture include the cloud "shared responsibility model" and the principles of "zero trust architecture."

Media play an important role in democracy to make people aware about information related to government policy and what the grievances people have but now a day media encroaches on public life, no one"s personal information is kept secure for their own interest [4].

Well-designed cloud security architecture should be based on the following key principles:

- **Identification**—Knowledge of the users, assets, business environment, policies, vulnerabilities and threats, and risk management strategies (business and supply chain) that exist within your cloud environment.
- **Security Controls**—Defines parameters and policies implemented across users, data, and infrastructure to help manage the overall security posture.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, April 2023
Impact Factor: 7.301

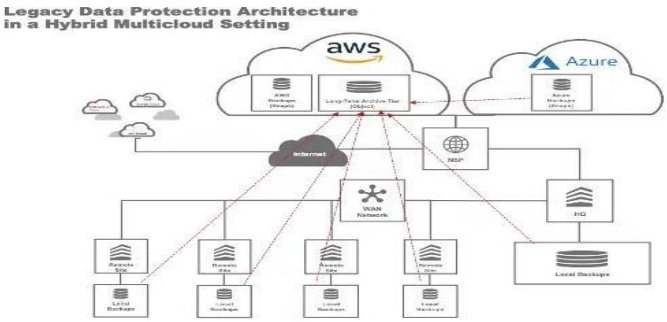


Figure 2: Principles of Cloud Security Architecture

- **Security by Design** - Defines the control responsibilities, security configurations, and security baseline automations. Usually standardized and repeatable for deployment across common use cases, with security standards, and in audit requirements.
- **Compliance**- Integrates industry standards and regulatory components into the architecture and ensures standards and regulatory responsibilities are met.
- **Perimeter Security**—Protects and secures traffic in and out of organization‟s cloud- based resources, including connection points between corporate network and public internet.
- **Segmentation**—Partitions the architecture into isolated component sections to prevent lateral movement in the case of a breach. Often includes principles of „least privilege‟.
- **User Identity and Access Management**—Ensures understanding, visibility, and control into all users (people, devices, and systems) that access corporate assets. Enables enforcement of access, permissions, and protocols.
- **Data encryption**—Ensures data at rest and traveling between internal and external cloud connection points is encrypted to minimize breach impact.
- **Automation**—Facilitates rapid security and configuration provisioning and updates as well as quick threat detection.
- **Logging and Monitoring**—Captures activities and constant observation (often automated) of all activity on connected systems and cloud-based services to ensure compliance, visibility into operations, and awareness of threats.
- **Visibility**—Incorporates tools and processes to maintain visibility across an organization‟s multiple cloud deployments.
- **Flexible Design**—Ensuring architecture design is sufficiently agile to develop and incorporate new components and solutions without sacrificing inherent security.

Social Challenges

- Principle says that people are the weakest link in Information Security.
- In Indian scenario people play vital role, people are the policy maker who will decide and direct the path for any technology. Though the Privacy issue is not at pinnacle in our culture because people are least bother about their privacy and there is no scam till now that directly impact on privacy but it is well said that prevention is better than cure [3][7].

Why Companies Need Cloud Data Protection

- Many companies collect and store significant amounts of information, including sensitive data. Most of this data touches the cloud at some point, either during collection or in storage.
- Part of the reason for the growth of cloud-based data storage is that organizations are increasingly operating via web portals or are using software as a service (SaaS) offerings. Both of these require cloud access. Additionally, many companies are choosing to store data in the cloud even for internal use.
- As companies adopt cloud services, data protection becomes more complex:
- Companies may not know where all applications and data are stored.
- Third-party hosting limits visibility into data access and sharing.
- Shared security responsibilities may be misunderstood or misapplied.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, April 2023
Impact Factor: 7.301

- If companies are using multiple cloud providers or hybrid infrastructures, security may be inconsistent.
- Data may be subject to data protection regulations like the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), or the USA Health Insurance Portability and Accountability Act (HIPAA).
- Data Protection Challenges in the Cloud
- When setting up data protection in the cloud, your organization is likely to face several of the following challenges:
- Integrity—systems need to be designed to ensure that only authorized access is granted. Configurations should also ensure that permissions to modify or delete data are restricted to appropriate users.
- Locality—data regulations are applied by the physical location of data, where it is collected, and where it is used. In a distributed system, this can be difficult to determine and control. Systems should be designed in a way that clearly defines where data is located at all times.
- Confidentiality—data needs to be secured according to its confidentiality level. This requires properly restricting permissions and applying encryptions to restrict readability. Likewise, admin credentials and encryption keys need to be protected to ensure that these restrictions are maintained.
- Storage—cloud infrastructure is entirely controlled by the vendor. This means that companies must rely on vendors to ensure that physical infrastructures, networks, and data centers are secure [6].

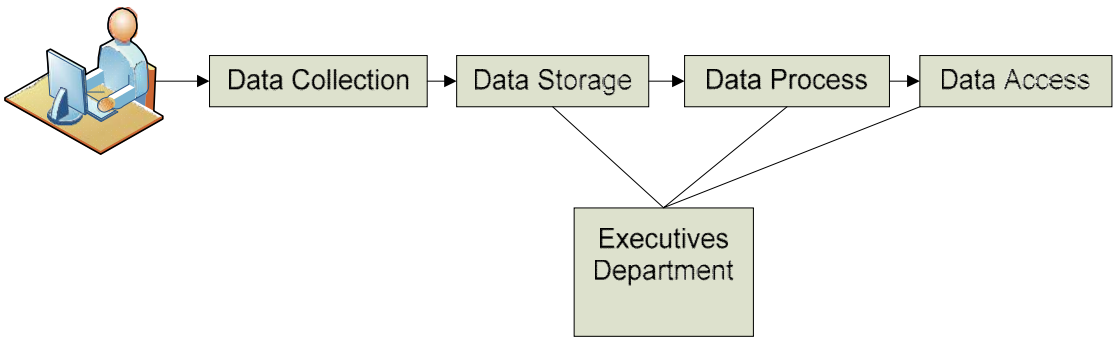
V. PROPOSED FRAME WORK

To observe privacy In Indian work culture we have to adopt above framework which clearly define general guidelines of information addressing in different phases. In this we cover all the necessarily measures while considering the threat to privacy and try to remove vulnerability present in the system. This model mitigates the risk to privacy to the appetite level. So that further threaten to privacy will reduce its impact. We divide the privacy protection in four phases Data Collection, Data Security, Data Process, and Data Access which describe are as follows.

5.1 Data Collection

- First step of privacy protection is start with data collection itself, there must be strict data collection policy impose by the top authority which clearly mention the following points
- Information is collected by authorize appointed agency only.
- Information is collected for lawful purpose only.
- Personal data shall be adequate, relevant and not excessive.
- Purpose of information collection must be mention.

If we capture the information properly then it is easy to maintain the information security in next steps. Government shall authorize the agencies for data collection government must also insure that they follow the regulation by doing periodic audit. Whenever information needs for collection it must be collected for lawful purpose only its commercial use is strictly avoided.



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, April 2023
Impact Factor: 7.301

5.2 Data Security and Storage

After data capture, personal data shall be kept accurately and kept up-to-date. Appropriate technical and organizational measure shall be applied. Technical measures include all information security controls which are necessary to keep information security over internet. If data is store on the server then that server must be fully controlled by government of India. Server must be taken all security safeguard against unauthorized access, use and other modification. Organization measure includes classification of information according to its nature.

5.3 Data Process

Personal data shall be process fairly and lawfully here processing means not only computer processing. We have to process data only when the consent of user is involved, if the user is in contract and one of the party of the contract, process if it‟s required for judicial proceeding, process if its legitimate use for national interest, process if it‟s vital interest of data subject. Data should be process for only given purpose. After processing, the data must be properly disposed. Retention policy must be specified as including purpose and duration of retention.

5.4 Data Access

The data access must follow Need to Know Basis. There must be control that information not goes beyond the Indian Territory. If data is going beyond territory then appropriate control must be taken to ensure that information is protected outside the India, there must be legal obligation between two countries about data handling. Within the country any Indian or non- government industry process the data they must have to follows all above the norms followed by the Indian government.

VI. RESEARCH FINDINGS

6.1 e-Governance

There is unique privacy challenges associated with e-governance due to large storage of personal and sensitive data. Obviously e-governance has given new dimension to development and globalization but there should be systematic improvements in governmental privacy leadership; and other technology-specific policy rules limiting, how the government collects and uses personally identifiable information. Government also has unparalleled opportunity to lead by example, by establishing strong, consistent rules that protect citizens without harming the government's ability of functioning. To achieve the specified goal we have to follow certain guidelines like:

- Creating a Union Chief Privacy Officer
- Installing chief privacy officers (CPOs) at all major departments
- Ensuring that Data Mining techniques are addressed by the Privacy Act
- Strengthening and standardizing privacy notices including "privacy impact assessments"
- Privacy Protection on agency website
- Complaint processing in case of breach of privacy

6.2 e-Jurisdiction

Finally India got its first awaited model e-Court at the Ahmedabad City[4]. Evidently the implementation of e- court in India is in its commencing state .The issues like privacy are still untouched. Without substantiation of the standard of technological framework and processes used by e-courts, the system of certainty upon which the courts and law are based has the potential to become inherently uncertain. It will be better to embed the privacy frame work to e court instead of including it later .

The e-court must provide security and privacy of electronic filings. Court shall make any document that is filed electronically publicly available online.”

- There must be unified and coherent policy for the privacy protection and access rights.
- Except where otherwise noted, the policies apply to both paper and electronic files.
- The availability of case files at the courthouse will not be affected or limited by these policies.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, April 2023
Impact Factor: 7.301

6.3 e-Media

e-Media include television channels, radio, internet podcast, and all electronic journalism which are used by today‟s media. Main purpose of media is to bridge the gap between government policy and public grievances. As there is no information classification in India every information is floated over the media its adverse impact is seen at 26/11 incident all government moves are shown on TV channel which is used by terrorist as a feedback they make their attack strong [6].

Privacy is most concern about celebrities but media is big threat to their privacy every gossip of celebrity is become a Breaking new in most of the new channel. Casting couch is very popular tool used by media now a day which directly hammer the individual privacy. There is no guideline to handle this issue privacy frame will provide solution to solve this problem.

6.4 BPO

BPO is Business process outsourcing in IT/ITES industries. BPO play major role for revenue generation in India, complement to BPO there are other types of industries also well establish like KPO (Knowledge process outsourcing), LPO (Legal process outsourcing) and others this is majorly based on information processing. India's BPO industry grew 60 percent to US $6.6 billion in the fiscal year ending 31 March 2008, according to the National Association of Software and Service Companies, in New Delhi. India's business- process outsourcing, or BPO, industry says its security standards match the best in the world. There has never been a major instance of data theft in India. Nonetheless, companies in the United States do fear such an event, says Richard M. Rossow director of operations at the U.S.-India Business Council in Washington, D.C. The fear is "not because they are at a higher risk of such a thing taking place in India, but rather because public perception of sending work to India is so bad that it will take only one major event for the affected company to 'pull the plug' on their India data service venture [1] [3].

If we do not ensure companies about strong privacy protection framework, we will lose outsourcing sector. We still rely on some international standard but unless if we not have legal framework, it will difficult to safeguard stake holder interest. Privacy at work place is also ignored field, thousands of workers are work in the premises as „people are the weakest link in information security‟ there must be guideline at work place like cell phone are strictly avoided, prior screening of employee, all work under electronic surveillance, technology used to access employees computer.

6.5 Telecommunication:

Service providers (SPs) including Internet service providers, number-database operators, telecommunications contractors, emergency call persons; public number directory publishers, authorized researchers and their respective employees must protect the confidentiality of information. The use or disclosure of any information or document which comes into their possession in the course of business must be restricted.

6.6 Health

Health sector is the important concern in privacy. Your health information includes any information collected about your health or disability, and any information collected in relation to a health service you have received. Many people consider their health information to be highly sensitive. Before proceeding it is very important to consider what all the issues that come under Health Information are:

- notes of your symptoms or diagnosis and the treatment given to you
- your specialist reports and test results
- your appointment and billing details
- your prescriptions and other pharmaceutical purchases
- your dental records
- your genetic information
- Any other information about your race, sexuality or religion, when collected by a health service provider.

There is certain legislative framework also prepared in other countries for the privacy issue like HIPPA and PSQIA Patient Safety Rule made by US government.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, April 2023
Impact Factor: 7.301

Keeping all this in mind it is mandatory to have a proposed system of health domain that mainly focused on privacy from Indian perspective. We must have administrative safeguard, technical safeguard, physical safeguard that will clearly define policy and procedure to provide safety of patient information. It covers issues like- there must be supported proceedings in case if someone disclose health information without consent of patient, there must be a written set of policy procedure and designate a officer responsible for implementing the procedure, Policy must clearly define class of employees that are allowed to access Electronic Patient Health Information, access of equipment that contains sensitive information must be properly monitored and controlled, protect your system from direct view of public, before transmitting any information must ensure the authenticity of the other party.

6.7 e-Business

We need a privacy framework purely focused on e-business and cover privacy issues and provide legal assistance in case of any fraud, crime .Issues that are need to cover under privacy framework like proper storage of sensitive credentials like credit card, safe credit of money during online transaction, Confidentiality, Integrity availability, authentication of party must be ensured before beginning of transaction, Encrypt the data before transmission of sensitive information, Restrict access based on need to know basis, assign unique identification to the parties that are involved in the business for authentication purpose. Also maintain the policy that addresses e-business privacy.

VII. CONCLUSION

The proposed system covers all domains in three dimensions legal, technical and political .In proposed system it has been tried to cover various domains as per present scenario, keeping the fast advancement in technology and emerging domains in the mind. The proposed system has given scope of advancement so that without interfering in other domains new domains can be added. The proposed system has been kept flexible and scalable so that not only present need but future needs can also be accommodated. Well-structured framework for Privacy is definitely important for an individual but also for society as well as economic growth of country.

REFERENCES

[1]. http://en.wikipedia.org/wiki/Privacy
[2]. PRIVACY AND HUMAN RIGHTS http://gilc.org/privacy/survey/intro.html
[3]. Privacy-Enhancing Technologies—approaches and development http://www.sciencedirect.com/
[4]. Ponnurangam Kumaraguru, Privacy in India http://www.cs.cmu.edu/~ponguru/iaap_nov_2005.pdf
[5]. The Fading Norm http://iltb.apargupta.com/2010/03/the-fading-norm/
[6]. Privacy and emerging technology: Are Indian laws catching up?
[7]. Internet privacy http://en.wikipedia.org/wiki/Internet_privacy
[8]. ITA Act 2008 http://cactusblog.wordpress.com/2010/01/21/amended-it-act-2008/
[9]. EU Directives http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm
[10]. http://www.oecd.org/dataoecd/56/36/1922428.pdf