Chapter 13
Criticality of E-Privacy and Data Leakage Amid the Pandemic: Privacy-Preserving Techniques and Frameworks

Gaurav Roy
EC Council University, India

ABSTRACT

The global pandemic has led to an undeniable surge in using digital technologies due to the social distancing norms and nationwide lockdowns. Firms and organizations are conforming to the new culture of work and life. The use of internet services, digital devices, and cloud systems has seen surges in usage from 40% to 100%, compared to pre-lockdown levels. With the rapid growth of this technological use, people are exposing their digital assets, presence, and behavior out to the binary world where AI-driven data analysis algorithms, data-gathering systems, and spyware are continuously monitoring their behavior. These subconsciously exposed data are then carried forward for delivering customized ads and recommend features.

INTRODUCTION

In today's digital epoch, data has become an asset for every organization and is valued more than gold. Every organization thinks of preserving the organization's data + the client's data or consumer's data. Recent advances and trends in technology like sensors & IoT systems, cloud, data analytics, databases, Smart devices, etc., are plausible to collect data effectively and pervasively. Organizations are taking data through static apps, cloud-connected apps, web apps, websites, online services, ads, and other malicious content. This chapter will primarily focus on the impact of e-privacy caused during the pandemic.

DOI: 10.4018/978-1-7998-7188-0.ch013

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

THE DATA FLOW

The use of internet services, digital devices, and cloud systems have seen surges in usage from 40 percent to 100 percent, compared to pre-lockdown levels (De, 2020). With the rapid growth of this technological use, people are exposing their digital assets, presence, and e-behavior out to the binary world. AI-driven data analysis algorithms, data-collecting systems, and spyware continuously monitor user behavior. These subconsciously exposed data are then carried forward for delivering customized ads and recommend features. But people are not consciously aware of it.

According to some reports, due to lockdown and increase in remote working culture, people's credentials are experiencing data breach due to remote work, organization's data are getting compromised because of the employee's negligence. 76% of participants realized that remote work increases the time to identify and contain a data breach (IBM, 2021). Healthcare systems went digital due to the increase in the number of patients during this pandemic. Weak systems with lesser security tests led to the data breach. Cybercriminals are attacking healthcare systems - stealing patient records and selling them on the dark web against monetary benefits.

Even though people are working promptly on data security and privacy for the last 25 years, we are still facing difficulty in data security and privacy challenges (Tawalbeh, p. 2020). It is the attack surface that is spreading wider every day - because of the deployments of new data collection & processing devices like IoT systems, data monitoring apps, cloud, online services, web apps, websites, etc. In the subsequent sections, you will get to know the different data breach and e-behavior leakage mechanisms taking place behind our back. Also, we will stretch further to how cybercriminals and legitimate organizations are selling our data to the dark web. Next, we will discuss how surveillance in individual e-privacy is becoming a concern. Lastly, we will cover the prevention mechanisms and comprehensive solutions organizations are using for preserving data privacy. Let us now peep into each topic in detail.

DATA BREACH AND E-BEHAVIOR LEAKAGE

A data breach is a form of cyber-attack that might change the course of your life or change the revenue graph of any business. Yes, it's the most vulnerable and attractive attack that intentionally and unintentionally makes an attacker release private or sensitive credentials to any untrusted digital ecosystem. Through this process, the cybercriminal gains monetary and other benefits by leaking the sensitive credentials of the victim. You might have heard about sensitive data disclosure, unintentional information disclosure, massive data leak, info leak, delicate data spill, and terms like this. Yes, all of them belong to the data breach. Most organized crimes also leverage the use of data breaches. During this attack process, cybercriminals extract the protected and sensitive data such as credit card information, personal health information (PHI), financial records, Personal Identifiable Information (PII), trade secrets, bank details, project plans, stat reports, behavioral analysis data, and other vulnerable unstructured data, files, or documents.

More than 3.5 billion people parts with their personal and sensitive data compromised in the top 2 breaches of the 21st century. Many other data breaches were untold. Did you know, Covid-19 had also brought cyber pandemics. Since so many trades, communication, and sensitive synergies went online without significant blackouts or business repercussions has unknowingly invited cyber-terror. Digitizing everything and remotely managing it from home has enabled you to make mistakes more. It is allowing

5 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/criticality-of-e-privacy-and-data-leakage-amid-the-pandemic/286251

Related Content

Survey of Recent Applications of Artificial Intelligence for Detection and Analysis of COVID-19 and Other Infectious Diseases
Richard S. Segalland Vidhya Sankarasubbu (2022). *International Journal of Artificial Intelligence and Machine Learning (pp. 1-30).*
www.irma-international.org/article/survey-of-recent-applications-of-artificial-intelligence-for-detection-and-analysis-of-covid-19-and-other-infectious-diseases/313574

LSTM Network: A Deep Learning Approach and Applications
Anil Kumar, Abhay Bhatia, Arun Kashyapand Manish Kumar (2023). *Advanced Applications of NLP and Deep Learning in Social Media Data (pp. 130-150).*
www.irma-international.org/chapter/lstm-network/324566

Exploring the Utility of Emotion Recognition Systems in Healthcare
Dinesh Kumar, Bhawnaand Daogafu Gwra Narzary (2024). *Using Machine Learning to Detect Emotions and Predict Human Psychology (pp. 245-271).*
www.irma-international.org/chapter/exploring-the-utility-of-emotion-recognition-systems-in-healthcare/340222

A Review on the Use of Artificial Intelligence in Reverse Logistics
Abhishek Kumar Sinha, Sajan T. Johnand R. Sridharan (2023). *Encyclopedia of Data Science and Machine Learning (pp. 2954-2969).*
www.irma-international.org/chapter/a-review-on-the-use-of-artificial-intelligence-in-reverse-logistics/317727

Generating an Artificial Nest Building Pufferfish in a Cellular Automaton Through Behavior Decomposition
Thomas E. Portegys (2019). *International Journal of Artificial Intelligence and Machine Learning (pp. 1-12).*
www.irma-international.org/article/generating-an-artificial-nest-building-pufferfish-in-a-cellular-automaton-through-behavior-decomposition/233887