Enhancing Data Security By Enabling Tracking Mechanism

R. B. Mohan Kumar
SVS College of Engineering
Coimbatore, India

Abstract— With the emerging technologies and tools in the internet world every operation made easier but securing the data created by an organization or an individual becomes more and more complex. Though there are various levels of security being provided by different OSI layers, tracking a file or document within a system, network or outside the network becomes even more difficult. Most of the organizations officially uses various document editors to create, store and share their data or information. There is no tracking mechanism currently available in the market for the files that are shared over offline or online. To overcome these challenges and issues proposing a new system that implements few methodologies by enabling the document editors to keep track of the files which are being accessed and updating the same in a centralized system. Also, the system provides an encryption logic so that files cannot be accessed by any other editors.

Keywords— data security, data sharing, tracking, monitoring

I. INTRODUCTION

Information security handles the protection of digital privacy of critical data of businesses, organizations, and individuals. It includes various preventive methods for restricting unauthorized access to databases, systems, machines, and networks. Security measures include but are not restricted to data backups, encryption, DLP planning, digital rights management, and more.

As organizations invest in digital transformation there is strong recommendation for data privacy and protection. New and expanded data privacy laws with growing enforcement of user rights for appropriate data use are a challenge for today's enterprises, which have more data, more applications, and more locations than even before.

The California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR), along with other state, global, and legacy mandates, can impose significant penalties on organizations that fail to protect data and respond to subject access rights for appropriate use. Organizations need to understand their own data privacy risks and organize controls to reduce unauthorized disclosure of consumer's private information.

The traditional and standard ways for setting up the secured environment is described in Table 1

Steps for secured environment
Secure data backups
Improve password-based data protection
Consider the losses and outweighs of a system shutdown
Establish a data loss prevention plan
Use digital rights management tools
Rely on secure file-sharing services
Provide adequate physical security for your company data
Prevent dos and ddos attacks
Evade advanced persistent threats
Use secure application programming interfaces
Encryption and decryption mechanisms

Table 1:- Defined ways for secured environment

In recent times, there are various big organizations who had faced crisis due to data breaches and lot of investments are made in building a highly secured infrastructure. This investments and research will help the mindset of customers and stake holders to feel better. But what happened to those personal information and private multimedia files of customers which are already exposed to world.

In this study, we will show how to address such problems and fine a solution for already lost or breached data and files. The name of our project is Document Tracking Editor (DTE)

II. PROBLEM IDENTIFICATION

Rather than investing time and money in lot of encryption and well-equipped firewall systems, massive research and engineering team after the breach. Prevention is always better than cure. There are lot of technology giants [6] were involved in data breaches in modern world, some of these giants ran out of business after these incidents. [Table 2] describes the hit based on impact in dollars.

No	Incident / Involved Organization	Date	Impact
1	Yahoo	2013-14	3b user accounts
2	Marriott International	2014-18	500m customers
3	Ebay	May 2014	145m users compromised
4	Equifax	July 2017	143m consumers
5	Heartland Payment Systems	Mar 2008	134m credit cards
6	Target Stores	Dec 2013	110m customers
7	TJX Companies, Inc.	Dec 2006	94m credit cards
8	Uber	Late 2016	57m Uber users and 600,000 drivers
9	JP Morgan Chase	July 2014	76m households and 7m small businesses
10	US Office of Personnel Management (OPM)	2012-14	22m current
11	Sony's PlayStation Network	Apr 2011	77m accounts
12	Anthem	Feb 2015	78.8m customers
13	RSA Security	Mar 2011	40m employee records
14	Stuxnet	2005-10	Meant to attack Iran's nuclear power program
15	VeriSign	Full 2010	Undisclosed
16	Home Depot	Sep 2014	56m credit cards
17	Adobe	Oct 2013	38m user records

Table 2:- Data Breaches on Big Technology giants

III. RELATED WORK

Many researchers have suggested their work using data and security, most of these studies have been conducted recently, focusing on modern research and facts. Review of few is as below:

P. Ravi Kumar, P. Herbert Rajb, P. Jelcianac. [1] The authors in this work, explored the different data security issues in cloud computing in a multi-tenant environment and proposed methods to overcome the security issues. Authors have also described Cloud computing models such as the deployment models and the service delivery models. In any business or Cloud Computing data are exceptionally important, data leaking or corruption can shatter the confidence of the people and can lead to the collapse of that business. Currently cloud computing is used directly or indirectly in many businesses and if any data breaching has happened in cloud computing, that will affect the cloud computing as well as the company's business. This is one of the main reasons for cloud computing companies to give more attention to data security.

Lo'ai A. Tawalbeha, Gokay Saldamli. [2] Authors of this work have reconsidered the security and risk in the modern big data and cloud environment. The general public users and organizations to make their life easier started relying on latest technology for assistance. Earlier humans trusted pen and paper but in digital era humans trust the digital much more than anything. The authors have analyzed few areas where the current big data storage, processing, security can be improved together. After analyzing the existing or current architecture of cloud authors have brought a solution for big data storage. By analzsing the peer to peer computation in cloud systems (P2PCS) authors have proposed a solution for processing and analytics in big data. With these two solution authors have come up with a model called HMCCM (Hybrid Mobile Cloud Computing Model), this model is applied on a health care use case as a simulator. As a result, HMCCM had performed 75% efficient when compared with traditional cloud computing models. Finally, authors have enhanced the privacy and security measures by considering possible threats and attacks.

Hicham Hammouchia, Othmane Cherqia, Ghita Mezzoura, Mounir Ghoghoa, Mohammed El Koutbib. [3] In this work authors have done deeper analysis into data breaches and performed an exploratory analysis of hacking breaches over time. Data breaches represent a permanent threat to all types of organizations. Although the types of breaches are different, the impacts are always the same. This work focuses on analyzing over 9000 data breaches made public since 2005 that led to the loss of 11.5 billion individual records which have a significant

financial and technical impact. Also, since the most devastating breaches are hacking breaches, Authors had shed the light on type to unveil the most targeted organizations and examine how the interest of hacker's changes over time. On the other hand, the breaches caused by human factor are decreasing which can be explained by the awareness of employees and the application of security standards. This work would improve the state of knowledge about hacking breaches and help in securing organizations data by prioritizing the most attacked sector.

Apostolos Malatrasa, Ignacio Sancheza, Laurent Beslaya, Iwen Coisela, Ioannis Vakalisa, Giuseppe D'Acquistob, Manuel Garcia Sanchezc, Matthieu Gralld, Marit Hansene, Vasilios Zorkadis. [4] In this work authors have addressed the personal data breaches of cross border. This became more necessary after the first data breach on personal data (1st PAN EUROPEAN PERSONAL DATA BREACH). Specifically, these data breaching incidents are kept on happening in real world now and then though there are data protection rules in place. Authors have performed a study to understand where the problem is and as a result, they have found two things which are interesting. The reasons are lack of communication between data protection officers, adhoc process in data protection. To avoid these issues in future authors have proposed a systematic approach for data protection and a framework for efficient communication.

Tintswalo Brenda Mahlaola, Barbara van Dyk. [5] This work presents the reasons for archiving pictures and communication system for data breaches and also talks about intentional and un-intentional breaches. The Picture Archiving and Communication System (PACS) has led to an increase in breached health records and violation of patient confidentiality. Objective: The purpose of this paper is to explore the nature of and reasons for confidentiality breaches by Picture Archiving and Communication System(PACS) users in a South African context. Authors have used the methods of questionnaire for collecting quantitative data from 115 health professionals employed in a private hospital setting, including its radiology department and a second independent radiology department. The questionnaire sought to explore the attitudes of participants towards confidentiality breaches and reasons for such behavior. As part of this exercise it resulted as breach incidences were expressed as percentage compliance and classified according to the nature and reasons provided by Sarkar's breach classification.

Cross tabulations indicated a statistical significance ($p<0.00$) between the expected and observed confidentiality practices of participants and also the adequacy of training, system knowledge and policy awareness. Hence, the study supports previous findings that, in the absence of guidelines, most security breaches were non-intentional acts committed due to ignorance. Of concern are incidents in which sensitive information was intentionally shared via social media.

IV. SECURITY ISSUES

The world loves sharing data and also they share it through several medium, highly categorized into two forms.

1. Online
2. Offline

When the data is shared only through the online like mail, online storage its trackable but it does not stop there it can again be shared through multiple other mediums, which is impossible in tracking the data. Most of the confidential information is stored in plain documents like text, docx, odt and much more. Some organizations follow strict rules like not to share any documents apart from organization's network. Intentionally or un-intentionally employees tend to make mistakes, but these mistakes incur high cost to recover or sometimes impossible to recover. Once the data breached no one can track who all have accessed and its definitely crucial to measure the impact. Its nearly impossible to measure the impact without knowing who have accessed and where the data is accessed.

V. DATA IS GROWING

The world is advancing with new technology on every day. *Technology is evolving!!! World is advancing!!! Data is growing!!!.* On every enhancement in technology security has to be

redefined. Public needs the quality of data to be very high it could be image recorded by handheld mobiles, digital cameras, high definition videos that are being played in online portals.

Due to increased quality the size of data that is being generated is also high. These quality files need huge storage capacity on a long term. Due to space constrain common public upload their personal and confidential data, pictures, videos into several cloud services which are cost effective. Everything is digitalized like medical reports is shared through mobile applications for easy access and immediate availability and easy access and industries does not stop there. These are several reasons why securing the evolving data is more necessary as world moves forward.

VI. FUNCTIONALITY REQUIRED

Based on all the issues that the organization is facing in the recent time we have prepared an approach that should have following functionalities [fig-1] to secure the highly confidential and private documents, so that the document owner or the organization will have full control over the shared document and the data reside in it. If we have a tool that has functionalities like send alert to the organization or the owner whenever the respective document is accessed, updated it will help the owners to be aware that breach is happened. So that they can act accordingly.

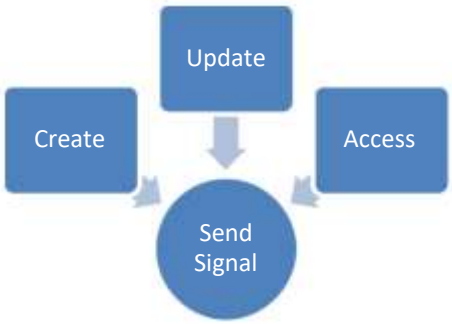

Fig 1 :- Functional Process

But then the data is already accessed, if the alerting team delays the severity increases, to overcome this issue there should be a file format encoding which cannot be accessed without the tool DTE (Document Traceable Editor).

Every document getting created should have unique key that should be synced in the organization server. So that out of the organization the document should not be accessible. Using this unique key, the document should be encrypted. If the user needs to remove several files from unauthorized access the user portal will provide remote delete option. This way everything is secured and tracked.

VII. PACKAGE DESIGN

As per the functionalities identified the system will have 3 integrated sub-systems for file editing, tracking and log analytics which is represented in [fig-2].

Fig 2:- Packaged System

File Editor: Provides the functionality for creating, updating or editing, saving and accessing the file. Tracking System: As a integrated part of the tool this will act as admin panel where alerts and signals will received from File Editor based on based on event. Log Analytics: This provides the insights about how many files are getting created, accessed and much more.

VIII. CONCLUSION & FUTURE WORK

There are many open source applications available for document work like Abi word, Libre Office, IWork. Integrating the tracking system and log analytics modules with any of these open source packages will provide a high end, efficient and rich document editor for users across the world. In case of cloud systems sharing and tracking data should also be thought. The current functional system mostly designed to work with standalone systems. Design has to be updated to configure the secured sharing environment in cloud, hybrid and mobiles devices.

REFERENCES

[1] P. Ravi Kumar, P. Herbert Rajb, P. Jelcianac, "Exploring Data Security Issues and Solutions in Cloud Computing", 6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017, Kurukshetra, India

[2] Lo'ai A. Tawalbeha, Gokay Saldamli, "Reconsidering big data security and privacy in cloud and mobile cloudsystems", Journal of King Saud University –Computer and Information Sciences

[3] Hicham Hammouchia, Othmane Cherqia, Ghita Mezzoura, Mounir Ghoghoa, Mohammed El Koutbib, "Digging Deeper into Data Breaches: An Exploratory Data Analysisof Hacking Breaches Over Time", International Symposium on Machine Learning and Big Data Analytics for Cybersecurity and Privacy (MLBDACP)April 29 May 2, 2019, Leuven, Belgium

[4] Apostolos Malatrasa, Ignacio Sancheza, Laurent Beslaya, Iwen Coisela, Ioannis Vakalisa, Giuseppe D'Acquistob, Manuel Garcia Sanchezc, Matthieu Gralld, Marit Hansene, Vasilios Zorkadis, "Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities", computer law & security review 33 (2017) 458–469

[5] Tintswalo Brenda Mahlaola, Barbara van Dyk, "Reasons for Picture Archiving and Communication System (PACS) data security breaches: Intentional versus non-intentional breaches", Health sa Gesondheid 21 (2016) 271-279

[6] Biggest Data Breaches of 21st century, https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html