Middle East Research Journal of Humanities and Social Sciences
ISSN 2789-7761 (Print) | ISSN 2958-2040 (Online)
Frequency: Bi-Monthly
DOI: 10.36348/merjhss.2023.v03i01.001

KUWAIT SCHOLARS PUBLISHER
Website: http://www.kspublisher.com/
Email: office@kspublisher.com

An Insight into Data Breaches: Challenges and Prevention

Dr. Pradip Kumar Das[1]
[1]Formerly Associate Professor, J. K. College, Purulia, S. K. B. University, Purulia, West Bengal, India

Abstract: Data breach is a deliberate or desultory denudation of classified materials to proscribed bodies. In the fast- evolving technology era, data has evolved into one of the most core elements of an organization. Data spill causes grim impendence to organizations and tarnishes its solvency. As the volume of data is flowering wantonly and data breaches are happing spasmodically all the more, diagnosing and forestalling data breaches have been one of the most crying invincibility presentiments for organizations. Despite copious exploratory studies on safeguarding sensitive information from being divulged, it remains a dynamic research theme. A clear-sighted methodology for data breaches management is the crying need of the hour and, hence, there should be sincere efforts to manage the problems. Against this backdrop, this paper on the strength of secondary data is a proposition to illuminate the concept of data breaches and their classification. This paper also appraises the gravity of data breaches and the challenges that need to be cogitated in the high-technology epoch.

Keywords: Data breach, Data security, Data breach prevention, Cybersecurity, Threat.

Research Paper

***Corresponding Author:**
Dr. Pradip Kumar Das
Formerly Associate Professor, J. K. College, Purulia, S. K. B. University, Purulia, West Bengal, India

How to cite this paper:
Pradip Kumar Das (2023). An Insight into Data Breaches: Challenges and Prevention. *Middle East Res J. Humanities Soc. Sci*, *3*(1): 1-8.

Article History:
| Submit: 01.03.2023 |
| Accepted: 19.04.2023 |
| Published: 30.04.2023 |

1. INTRODUCTION

Sprouting appositeness of information technology revamps consumer behavior, upgrowth of corporate strategy and communication. Technology fads like internet, artificial intelligence, machine learning and developing capillarity of the rocketing connection speed produce substantial insights on security data (Newman, 2019). As the relationships between consumers, organizations, governments and other entities become prominent, consumers should be observant about purport of data (Panetta, 2018). Trailing multiple cyber-attacks, organizations encounter viable exigency and also honor the surfacing directives about data protection (Kammel *et al.*, 2019). Governments are accrediting new percept to protect consumer's secrecy while the regulatory bodies are seeking to cultivate limpidity following milking stern guidelines e.g. demanding disclosure of data breaches, exacting high retribution for violating confidentiality to protect data. Despite all endeavors to safeguard operations, data breaches have become almost common in organizations. However, major fallibility is threat to privacy, integrity and security of data. Organizations find it challenging to secure their data and necessitate to exert multiple technologies for the betterment of efficiency. Hence to assure information security and mitigate gamble of data breaches, organizations must adopt modish recipe towards the flowering of safe, prophylactic and stable mechanisms. In this context, this paper is a modest attempt to feed decipherment of data breaches, its challenges and preventions.

2. Problem

Data breach is a staid menace to business procedures like corporate body and administration. Dispossession of off-the-record materials can besmirch and even are nocuous to the strength of an organization. Lately, there appears many conspicuous data breach episodes that impact organizations prodigiously. Since infobesity is springing exponentially in the digital world and data breaches betide much still more, extricating and precluding classified data from being tattled to interdicted crews becomes one of the most burning aegis perturbations for organizations.

3. OBJECTIVE OF THE PAPER

The basic objective of this paper is:

i) To examine the concept of dealing with data breaches in the age of fast-evolving technology;
ii) To discuss the major causes of data breaches;
iii) To detail the various classes of data breaches;
iv) To finalize with a discussion of data security measures that can be used to prevent breaches.

4. MATERIALS AND METHODS

The study is descriptive in nature and conducted by variety literatures apropos data breaches, its causes and prevention. Descriptive research has been preferred for developing better profundity of knowledge. Thus, this study purely adopts secondary data collection strategy, and considers a variety of secondary sources accessed through the Internet and academic databases viz. literature reviews, empirical studies, website, books, journals, reports, etc. The work is designed for a cross-section of those for making the issue easily understandable and organized into several sections. Besides, the paper being descriptive and conceptual in nature, the opinion expressed in this paper is author's own opinion and thought. The inherent limitation of the study is that as the study is based on published data and information, and this secondary source may be lacking in authenticity, the result inferred therefrom may not be completely reliable. The corpus of this paper is, therefore, limited to establish, in the first place, a global sketch on data breaches. In the second place, an assessment on the foremost mission endeavoring discernment of the impact of data breaches on organizations has been delineated.

5. Data Breaches-Concept

Data breach is an incident where sensitive data are ignobly divulged either wittingly or unwittingly by intruders or by meticulous group of miscreants whose intent is money (Chen and Zhao, 2012). Usually, illicit individual essays to encroach data of closet, company shares, business specifics or legit materials. Data breaching mainly subsumes phishing, denial of service attack, malware and exfiltration. This is mingled with crucial information e.g. credit card numbers, CVV code, social security numbers, password, medical history and insurance setup. Data breach often thrives without proper security measures. Besides, data breaches fire at large corporations earmarking customers list, product source code, trade secrets and deposit summary. Data breach represents perennial ambushment to organization. Without felicitous venture to ameliorate disaster recovery, business may flunk to restore its responsibilities. Convulsion in the running of system hardware and crumbling system software is also significant. Novel methods can better sustentation of data. Cyber Threat Management (CTM) impedes data breaching. Although there appears headways of melioration in preventing data leak, there are many possibilities of theft and its consequences. Portents may originate from multiple dawns like natural catastrophe and high-tech debility. Political dogmatist or company's contestant can also intimidate. Further, miscreants may conceivably be member of the same organization and attempt to conglomerate dealings confidence, furtive matters, network, security information, etc.

6. LITERATURE REVIEW

Over the years, a number of studies have analyzed the issue of data breaches and offered solutions. Marcus (2018) appraised insightful explication to safeguard consumer's data gathering through framing security standards, codification of privacy and introduction of personal identity setup and modulation of public identity numbers. Jang- Jaccard and Nepal (2014) accepted corporality of security vulnerabilities debilitating interpretation of data. Security of data stands on three essentials i.e. probity, taciturnity and accessibility. The study prescribed few measures to expropriate data breaches like data encryption, embracement of intranet, decryption and network IDS. According to the 2005 computer crime and security survey by CSI/FBI, 95% respondents disclosed that their organization experiences more than 10 Website incidents in 2005 against only 5% respondents in 2004 (Gordon L. *et al.,* 2004 and 2005). Garg *et al.,* (2003a) estimated that on average, security issues cost breached companies 0.5% to 1% of annual sales. The authors also reviewed spillover effects on security vendors and insurance carriers, and observed that share prices increase between 1% to 3% and 1% to 2% by security vendors and insurance carriers respectively for security breach. Hovav and D'Arcy (2004a) surveyed implication of virus outbreak promulgation. The authors identified no unpleasant outcome over five days following the event. However, they noticed almost half of the firms experienced unpleasant outcome over twenty five days after the notification. Cheng *et al.,* (2017) proposed a number of protective umbrellas for data breach like initiation of network IDS, data coding and encapsulation. According to a survey**,** out of 410 IT decision makers, about 75% shared that IT security has been captious to their planning and over 80% declared that they are involved in dire straits (Muncaster, 2006). Studies exercising event study methodology observed business response of data security dereliction (Campbell *et al.,* 2003; Cavusoglu *et al.,* 2004; Garg *et al.,* 2003b; Hovav, 2003a and 2004b). Cavusoglu *et al.,* (2004) observed that security breach proclamations impact the breached firms and internet security pioneers. The breached firms missed 2.1% of their market value within two days following the public announcement. Security pioneers realized freak return of 1.36%. Average loss from the illicit rights to information has swelled to $300K from 51K and loss from the extortion of trade secret has also risen to $356K from $169K since 2004. Thus, data breach causes tremendous financial drops to organizations (Egan and Mathen, 2005; Warren and Hutchinson, 2000). Hovav and D'Arcy, (2003b) in their investigation on the impact of denial-of-service (DOS) attacks by reviewing stock market response observed trivial effect of DOS attacks on capital market. However, their results focused trifling financial impact on internet-specific companies. Thakur *et al.,* (2015) excogitated perception of cyber-crime and its implication on data protection. The paper proposed few measures in cultivating data protection. Trivial means to encounter data breaches are induction of firewalls, embracement of security software and balking

passwords. Campbell *et al.,* (2003) examined stock market repercussion of data security breaches on public enterprises and found significant oppugning response. The authors concluded that economic implication of security breach stands on essence of breach. However, the study also demonstrated that market is sensitive to other categories of security breaches.

7. RESULTS AND DISCUSSIONS

7.1 Data Breach–its Relegation

Relegation of data breach threats builds on its motivation divulging insightful clue. Both insiders and outsiders can embarrass exposure. Hacker break-ins, malware, virus, social engineering, etc. normally create external data breaches. An adversary can manipulate a system cryptoware or sophistical admittance controls to circumvent server's documentation device and login to embarrassing details. Social engineering attempts become crescively pragmatical by jesting individuals into transmitting valuable company data to cyber criminals. Internal data exposure is imputable to either deliberate actions or inadvertent mistakes. Hauer, (2015) proposed comprehensive criteria for portraying 1259 data leakage prevention (DLP). The results disclose that both technological and non-technological aspects can arrest data breaches. Identity Theft Resource Center (ITRC, 2017) reported that total number of major data breach experiences keeps increasing. Data breach incidents are 40% more in 2016 than 2015. Business and healthcare leaks take majority. In 2016, business data breach has 494 reports taking 45.2% of the overall breaches followed by healthcare representing 34.5% of the overall breaches with 377 incidents. Data breach by collocation of phenomenon occurs mainly by internet exposure or employee mistake. Malicious outsider in 2016, purloins around 55% of the overall breach incidents. However, the reports provide different results for employing nonidentical data sets and confirm that insider threats emerge as the leading cause of enterprise data breach threats. Relegation of organization data leak threats is as: **Intentional threats:** i)Malware; ii)Hacking; iii)Cyber espionage; iv)Social engineering; v)Trojans; vi)Sabotage; vii)Virus and **Inadvertent threats:** i)Improper encryption; ii)Configuration error; iii)Lost computer; iv)Accidentally publishing; v)Privilege abuse.

7.2 Data Breach-its Classification

Ransomware, the fastest-growing form of data breaches embroils felonious molester encrypting files and intimidates target organization into squaring money. Molesters threaten to wreck critical data whenever affected organizations muff extortion demands. The best form of ransomware delivery system is phishing spam attachment through email disguising. However, once file is downloaded, molesters expropriate victim's computer and ransom begins. Notwithstanding network's resilience, malware is planted in attachments sneaking past security firewall unnoticed. Access to computer files is a critical operation indicating that if molester occupies files, productivity halts costing firm millions (Bendovschi, 2015). Online accounts, emails or other services are mortally harmed for their relativities on intruded web. Smurf attack and SYN flood are two common tactics of service breach. In Smurf attack, criminal dispatches internet control message protocol broadcast packets to hosts with spoofed source internet protocol address of target machine. Recipient responds thereby being swamped with responses. However, SYN flood happens wherever molesters dispatch requests to link to victim's network server but fails to finish connection. Cybercriminals proceed to dispatch requests until all exposed ports drench preventing from communication (Seemma and Sowmiya, 2018).

Phishing collects delicate data of target victim by exercising deceptive websites and emails. Molesters adopt disguised emails as tool. Expressly, aim is to deceit victims on the plea that they need. It camouflages credible entity linked with victim. Emails are the most popular bit managing one for cyberpunk.

Malware insinuates numerous malicious software programs abused by cyber traducers. Malware intrusions having codes framed by molester for wide-ranging mutilation capture unauthorized ingress to network. Data breach is frequently relinquished through link over emails and awaits intellect to open file or click on link to execute malware. Molester utilizes malware to pilfer cryptogram from victim. Major Malware programs encompass worms, viruses, trojans and spyware. Virus is the most common type of malware and customarily connects malicious code and stays for robotic naive to implement virus. Spyware, instead, is fashioned to stalk movements of user. It curtains in the backcloth of computer and collects confidential data like credit card details, password, etc. (Valuch *et al.,* 2017).

Insider threat assists criminals for revenge or being blackmailed by molester. Few staff reciprocates when they feel despised or have been dropped. Staffs retaliate through periling organizational performances. Analogous staff grabbing data transmits them to dark web. Organizations attempt to avert this by allowing staff to firm's classified data. Molesters need not be current staff but may be former, business partner, consultant or board member. Major types of insider threats comprise pawns and turn cloaks. Pawns are not malicious but commit mistake allowing access to exploit or otherwise cultivate data leakage or adjustment. Workers fallibly email documents containing classified data to crook. Conversely, deceivers deliberately pilfer data from organization (Seemma and Sowmiya, 2018).

Physical theft is widerspread in multiple organizations. Molesters pilfer materials like paper records and devices containing off-the record data. This

happens when paper information is not properly scraped ebbing in the malicious persons. Molesters collecting information from discarded documents without tattering scoundrel employ it for malicious purposes. Organizations are enlivened to ware when chucking machineries like USB sticks and computers via cinching that everything is decimated from device. Physical theft can also eventuate when staff desert records and devices secluded palpably (Valuch *et al.*, 2017).

Employees are key defense gullibility for any organization. Organizations just click button. Employee dispatches bulk emails and handles Cc rather Bcc field thereby dispatching materials to felon. This is calamitous whilst documents contain state secret. Further, employees are conjointly culpable by committing mistakes espousing molesters to ingress into organization's privateness. An employee as well spuriously dispatches awry papers to deliberate person. Although it is frail humanity, employees have to contemplate key factors of data security (Bendovschi, 2015).

7.3 Challenges

Although upswing of electronic database begets overwhelming hopes, elephantine data breach incidents perforce have become peripheral nocuous for sprouting data within corporate systems. Outcomes of individual data breach spawn millions of people's information and suffer delinquency. Most often, embarrassing data are encountered among varied stakeholders. Cloud file sharing and outside interaction metamorphosing ubiquitous for organization exacerbate data spill subject. However with squirming of manpower, staff working from outside multiplies data breaches. Further in big data environments, stimulus behind cyber-attacks on filching private data skyrockets with big revenues. These aspects maze core challenge of encountering supposititious operation and divulgence of confidential data. Detection of inside data encryption flukes is incredibly arduous since internal breaches often embroil freaks having licit gateway to data. Virulent staffs outflank organizations safety strategy by stashing sensitive data and radiating them via furtive channels. To prevent inadvertent data breach, it is imperative to accelerate security sensibility in workspace. Here, few challenges for data breach detection are outlined below:

- **Scalability:** Potency to process gigantic volume can be deployed in distributed environments where third-party owns manipulating knobs. Scalability is key to elutriating substantial organization data. A protractile key can disrate data storage setback and score rapid data breach detection.
- **Confidentiality:** Ingenuity to sustain confidentiality of sensitive data from intruder despoiling the exposure is vital. Privacy is a bigwig during deploying data breach detection to third party.
- **Meticulousness:** Distributed nature of big data environments constitutes challenge in definite leakage detection. Outsourced data to third-party may be refashioned via disparate freaks lowering veracity of content-based approach.
- **Alacrity:** Pronto, detect and react to data breaches before catastrophe. Diversity and celerity of big data breed opportunities and also challenge for real-time identifying data breach threats.

7.4 Common Reasons for Data Breach

i) **Staff's Error:** Staff's practicing poor code may share a organization's practice to successive affront.
ii) **Malware:** Hackers use catty software e.g. spyware, viruses, adware, etc., to grab confidential details from an organization's network system. It is inexorable to still its recrudescence whenever organization flunks to escalate monitoring etiquette after its initial breach.
iii) **Early Susceptibility:** Hackers usually dump a dripstone they can use to wriggle in organization's practice de novo after a thriving first stab. Dereliction to replenish susceptibilities from the maiden ambush precipitates a second one.
iv) **Others:** Other errors have staff clicking on virulent links and surveying phishing sites. Staff can reiterate early missteps that elope organization unscreened except it executes security training after initial breach.

7.5 Preventive Measures

Notwithstanding the essence of technical innovation for preventing data breaches, hackers still initiate blitzes by milking the fallibilities in electronic network of organizations or their staff. Various measures adopted for management of data breaches can be categorized into technical, organizational, policies and standards (Lykou *et al.*, 2018). Cybersecurity provides impedance of data sprinkle. Since the number of data breach is skyrocketing, preventing data breaches has become the crying need of the hour. Data security techniques play vital role to oust the threats of breaching.

i) **Technical Practices:** Organizations should enact clamorous technological etiquettes like firewall setup and network architecture. Network infrastructure should be protected from illegitimate access. Firewall permits or averts access into network. Anti-malware program is another technical strategy to manage data breach. All computers acclimated for data storage should have running anti-malware software to protect malware and ensure protection of data integrity. Safe data reckons on satisfactory Intrusion Detection System (IDS) that detects malicious activities, but experiences high false positive rates (Julisch and Dacier, 2002). This system eyes computer and network operations to search proscribed encroachment. Strategy surveys hardware and also

software systems of network (Liao *et al.,* 2013). Issue can be escalated and prevented betimes with such strategy. Data safety having dependent on data encryption forestalls intrusiveness during dissemination approach over accessible web. New tools for safeguarding confidential files on computer rest on digital machine (Borders, *et al.,* 2009). Strong user authentication can protect data breaches. Unique password is a common technique to create user authentication and prevent illegal bypass into key information (Kong *et al.,* 2018). Management should develop appropriate framework to frame Bring Your Own Device (BYOD) and security policies for preventing employees from subsuming their personal devices into organizations systems. Trusted computing techniques offer digital-based cradle of certainty for scoring core defence (Alawneh and Abbadi, 2008).

ii) **Policies and Standards:** Organizations should arrange for specialized info security training. Besides, it should enforce specific rules in the deployment of software, and also lay standards in hiring and selecting security officers having aptitudes to encounter data security. Organizations must cultivate culture of continuous monitoring of data security and not wait for walloping to surveil the degree of data security.

iii) **Organizational Practices:** User access management is a core component in managing data breaches. This practice can be bagged through educating the patrons on how to ensure top-level of security (Chen & Zhao, 2012). Besides, proper user training measures may be adopted to encounter patrons who are unaware of anti-malware programs. Organizations should introduce frequent employee training and proper data storage system to handle any growth of data and also ensure access management before endorsing to systems.

Few trivial contrivances to prevent data breaches:-

i) **Breaching response:** Instituting breach response plan helps dispatch admonitions to management by notifying about attacks and thereby lessens outrage of data breaches.

ii) **Banning unencrypted devices:** Unencrypted devices are more vulnerable to data leakage. All unencrypted portable devices practiced in organization are to be verboten.

iii) **Shredding files:** Shredding files, folders and disks engross expunging data files permanently without retaining a copy of the same. Thus, shredding of the confidential data prevents data breaches.

iv) **Robotic security:** Exercise of automated systems for conforming password clamping, server and firewall configuration lessens risk of data breaching.

v) **Spastic password:** Securing password is hard to crack and unpredictable to prevent illegal access of data. Password can be evolved methodically.

vi) **Protecting data:** Sensitive information requires protection and not exposure unwittingly.

vii) **Restricting download:** Restrictions on downloading confidential data lower chances of transmission to external device.

viii) **Reducing data transformation:** Proscription of migration of data from one device to another in organization is a bold step since loss of removable media wreaks data in jeopardy.

ix) **Red Seal:** Red seal addresses firewall complications. Firewall halts blending of secured network and unsecured network. All network elements transfer their data to Red Seal. It is an elongation of routine engineering and spurred by red seal.

x) **Contrast Security:** To prevent false forging, agents of contrast security are embedded into application program which becomes intrinsic. Contrast security has experienced significance without generating data breaching on Open Web Application Security Project (OWASP) security standards. All normal apps are metamorphosed into applications which are destined on security.

xi) **Crossbow:** Crossbow is the most protective strategy against frangibility and contributes sensivity proof for assessment. Earthshaking intrusion can be emplaced for vulnerability by exposing to secure grid.

Cyber Threat Management (CTM) is an important tool to predict threat before occurrences. CTM encompasses: i) Automated intelligence; ii) Threat analytics; iii) Cyber threat hunting; iv) Advanced analytics and security intelligence; v) Rapid decisions. CTM precipitates safeguarding software.

8. RECOMMENDATIONS

i) Data breach prevention software helps organizations distill data traffic, arrest key data and protect ceiling from being trapped cattily.

ii) Executives of organizations should upgrade their data security methodology for regulation, transmission and upkeep of corporate information. Lest, creativity and spirit of employees demote.

iii) Planning and devices ought to be pliable and seasoned to observing inside and outside the organization to sight and allay commination to information security.

iv) Scanning data stored in servers accredits to detect budding data breach risks inside organization. Monitoring averts inept practice of sensitive data and obstructs them from passageway towards corporate network.

v) Organizations must savvy clouds stuck with crypto currency theft. Exquisite course to

protect against this fraud is to guarantee that each sensitive data is encrypted.

vi) A holistic approach helps study countries adopting National Institute of Standards and Technology (NIST) framework and International Organization for Standardization (ISO) standards or relevant local regulations. Deliberation on how particular countries apply standards to local organizations facilitate in acceding degree of data security regulation.

vii) No organization should renege its security standards.

viii) Cardinal disposition of prescient security defenses enlightens asperity level of intrusion and lowers data flow risk.

ix) Innovation and practices must be associated with staff training. Staffs are cognizant of attempts and can withstand against them. Invincibility bets on ongoing learning of staff about detecting skeptical dissemination and novel plausible crisis.

x) Executive managers must cultivate a culture of trust to alleviate cyber-threats because insider mistakes are insubstantial and usually indiscernible. Defence measures are decisive to epitomize data breaches and insider lapse.

xi) Organizations need top-notch security to impede political attacks because not all breaches are fomented by returns.

xii) Healthy patch management strategy and constant gullibility evaluation help prevent outside molesters with several layers of security using anti-virus solutions, network behavior search and log supervision. It is significant for an organization to scape extemporary running of sensitive information.

xiii) Organizations require enlightened stewardship to revamp technology and to substantiate that internal human factors refuse data corruption.

xiv) In a mountingly globalizing world, a frail security standard favors to extend complying with other organizations despite their pursuing healthy standards. A regional setback sways all; thusly urgency for global policy for protecting data springs.

9. CONCLUSION

Data, now-a-days, is crescively becoming interlaced with business pursuits. Cybercriminals constantly evolve updated high tech measures to intrude illicitly into business system especially those with explosive details. Contemplating and forestalling data breaches necessitate ongoing strife from organizations. Cyber security is prognosticated to breed over time. The study contributes panoramic vignette of discrete stratagems. Decent approach must be insinuated to withstand breaches mustering organizational stratagem. Challenges demand more enthrallment principally in the robotics bout. Organization should ideally lucubrate to integrate the measures to establish best security in its approaches. Multiple roseate research briefings for downsizing data schism vulnerabilities in organic structure have also been insinuated. Prescriptions of data flow spotting as a cloud service and deep learning for insider threat are explicitly propitious. Lastly, data security environment would be more impervious wherever concept of artificial intelligence blossoms more-and-more in a wink.

10. Implication of the Study

Result of the study is worthwhile to feed executives, governments, regulators, corporate and virtuosos in the esoteric perceptive of protocol to be pursued for the evolution of prescriptive etiquette and organization's management for downsizing data spill issues and security flaws. This study also contributes to societal transition change through educating managers about circumventing data breaches who, in turn, can invoke information accessibility without retribution. Protecting confidentiality is a big challenge as one data breach can impact many and jeopardize viability of a sweeping organization.

11. Research Comments

Tragically despite dramatic growth in security defenses worldwide, data breaches are still a big exercise. Results demonstrate that the elucidations can arrest inadvertent data encryption while insiders or malware can deftly sidestep the protection by clouding data. Industrial elucidations are inadequate to protect against opprobrious data breaches. Although context analysis has the eventuality for remedy, cultivating potent insider detection systems bides a direct question. Despite a bellyful of research on data breaches, detecting and preventing organization data breaches is a simmering exploration dilema.

12. Research Scope

Till now, multiple research issues and scopes remain surreptitious. A few of them are:

i) **Cloud service:** Cloud service backer is an important research direction to attain scalability without lessening detection fidelity.

ii) **Paradigm for extrusion prevention:** With growth of robotics, academic research stipulates average datasets for assessment and complicates to associate with modern elucidation. Research community necessitates tools to boost data sharing and paradigm sensivity attempt.

iii) **Deep learning for insider risk espial:** In bulky database atmosphere, data mining and robotics tools divulge secret data leaks as also develop exactness and well-timed invulnerability. Training deep learners to extrapolate chains of user intent is a *riveting* dictum.

iv) **Surveilling encrypted approach:** Future research elucidation requires observing encrypted approach to encounter furtive data

leakage. Techniques in this locale may too be operated to encounter transmission of insightful data on encrypted channels.

ACKNOWLEDGMENT

I thank my ALMIGHTY GOD for sustaining me with HIS love, care and strength to enable me to walk through this journey.

REFERENCES

- Alawneh, M., & Abbadi, I. M. (2008). Preventing information leakage between collaborating organizations. *Proceedings of the 10th International Conference on Electronic Commerce, ICEC*, Innsbruck, Austria. New York, NY: ACM, 38:1–38:10.
- Bendovschi, A. (2015). Cyber-attacks- Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance, 28*, 24-31. doi: 10.1016/S2212-5671(15)01077-1
- Borders, K., Weele, E.V., Lau, B., & Prakash, A. (2009). Protecting confidential data on personal computers with storage capsules. *Proceedings of the 18th Conference on USENIX Security Symposium, Montreal*, Canada. Berkeley, CA: USENIX Association, 367–382.
- Campbell, K., Gordon, L., Loeb, M., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(2003), 431-448.
- Campbell, K., Gordon, L., Loeb, M., & Zhou, L.(2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(2003), 431-448.
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce, 9*(1), 69-104.
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce, 9*(1), 69-104.
- Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. *In 2012 International Conference on Computer Science and Electronics Engineering, IEEE, 1*(0), 647-651.
- Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions: Enterprise data breach. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7*(5), e1211. DOI:10.1002/widm.1211
- Egan, M., & Mathen, T. (2005). *The executive guide to information security threats, challenges, and solutions*. Indianapolis: Addison-Wesley.
- Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security, 11*(2/3), 74-83. DOI: 10.1108/09685220310468646
- Garg, A., Curtis, J., & Halper, H. (2003a). The financial impact of IT security breaches: what do investors think? *Information Systems Security, 12*(1), 22-33. DOI:10.1201/1086/43325.12.1.20030301/41478.5
- Garg, A., Curtis, J., & Halper, H. (2003b). The financial impact of IT security breaches: what do investors think? *Information Systems Security, 12*(1), 22-33. DOI:10.1201/1086/43325.12.1.20030301/41478.5
- *Gordon, L., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2004). CSI/FBI Computer Crime and Security Survey.*
- Gordon, L., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). *CSI/FBI Computer Crime and Security Survey*.
- Hauer, B. (2015). Data and information leakage prevention within the scope of information security. *IEEE Access, 3*(0), 2554–2565. DOI:101109//ACCESS.2015.2506185
- Hovav, A., & D'Arcy, J. (2003). The impact of denial of- service attack announcements on the market value of firms, *Risk Management and Insurance Review, 6*(2), 97-121. https://doi.org/10.1046/J.1098-1616.2003.026.x
- Hovav, A., & D'Arcy, J. (2003a). The impact of denial of- service attack announcements on the market value of firms. *Risk Management and Insurance Review, 6*(2), 97-121. https://doi.org/10.1046/J.1098-1616.2003.026.x
- Hovav, A., & D'Arcy, J. (2003b). The impact of denial-of- service attack announcements on the market value of firms, *Risk Management and Insurance Review, 6*(2), 97-121. https://doi.org/10.1046/J.1098-1616.2003.026.x
- Hovav, A., & D'Arcy, J. (2004a).The impact of virus attack announcements on the market value of firms. *Information Systems Security, 13*(3), 32-40.DOI: 10.1201/1086/44530.13.3.20040701/83067.5
- Hovav, A., & D'Arcy, J. (2004b). The impact of virus attack announcements on the market value of firms, *Information Systems Security, 13*(3), 32-40. DOI: 10.1201/1086/44530.13.3.20040701/83067.5
- Identity Theft Resource Center. 2017. http://www.idtheftcenter.org/. (Accessed March 1, 2017).
- Isaac, M., & Frenkel, S. (2018). Facebook Security Breach Exposes Accounts of 50 Million Users. *New York Times*.

- Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973-993. DOI: 10.1016/j.jcss.2014.02.005
- Julisch, K., & Dacier M. (2002). Mining intrusion detection alarms for actionable knowledge. *Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining,* July 23–26. New York, NY: ACM; 366–375.
- Kammel, B., Pogkas, D., & Benhamou, M. (2019). *These Are the Worst Corporate Hacks of All Time 18 de março*. https://www.bloomberg.com/graphics/corporate-hacks-cyber-attacks/
- Kong, W., Lei, Y., & Ma, J. (2018). Data security and privacy information challenges in cloud computing. *International Journal of Computational Science and Engineering, 16*(3), 215-218.
- Liao, H.-J., Lin, C.-H., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications, 36*(1), 16-24.
- Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Implementing cyber-security measures in airports to improve cyber-resilience. *In 2018 Global Internet of Things Summit (GIoTS),* 1-6.. DOI: 10.1109/GIOTS.2018.8534523
- Marcus, D. J. (2018). The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information. *Duke LJ, 68,* 555.
- Muncaster, P. IT Decision-makers more concerned about security, VNU Network, http://www.vnunet.com/articles/2150356 February, 2006.
- Panetta, K. (2018, October 15). *Top 10 Strategic Technology Trends for 2019.* https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/
- Seemma, P., & Sowmiya, M. (2018). Overview of Cyber Security. *International Journal of Advanced Research in Computer and Communication Engineering, 7*(11), 125-128. doi:10.17148/IJARCCE.2018.71127
- Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015). An investigation on cyber security threats and security models. *In 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing* (307-311). *IEEE.*
- Valuch, J., Gabris, T., & Hamulak, O. (2017). Cyber Attacks, Information Attacks, and Postmodern Warfare. *Baltic Journal of Law and Politics, 10*(1), 63-89. doi:10.1515/bjlp-2017-0003
- Warren, M., & Hutchinson, W. (2000). Cyber-attacks against supply chain management systems: a short note, *International Journal of Physical Distribution & Logistics Management, 30*(0), 710-716. DOI: 10.1108/09600030010346521
- Weise, E. (2016). 360 million Myspace accounts breached. *USA TODAY*. Newman, D. (2019, July 14). *Top 10 Digital Transformation Trends For 2020.* https://www.forbes.com/sites/danielnewman/2019/07/14/top-10-digital-transformation-trends for-2020/