JAGRAN JOURNAL OF MANAGEMENT AND TECHNOLOGY

ANNUAL PEER REVIEWED JOURNAL

VOLUME 5 | ANNUAL SUB. : Rs. 500 | AUGUST 2023 | ISSN. 2583-293X

JIM
JAGRAN INSTITUTE OF MANAGEMENT

Jagran Institute of Management

JAGRAN EDUCATION FOUNDATION

(Promoted Under the aegis of Shri Puranchandra Gupta Smarak Trust)

Jagran
An initiative of Dainik Jagran

Your future our goal .....

Pursuing Excellence for 25 Years in Education

K-12 Schools

- Puranchandra Vidyaniketan, Kanpur
- Jagran Public School, Noida
- Jagran Public School, Lucknow
- Jagran Public School, Varanasi
- Jagran Public School, Kannauj
- Jagran Public School, Basti

Jagran College of Arts, Science and Commerce, Kanpur

B.Sc (PCM), B.Sc (ZBC), BA, B.Com, BBA, BCA, B.Com (Hons.), M.Com

Contact No : 0512- 2647289

Website : www.jagrancollege.ac.in • **Email:** jagrancollegeasc@gmail.com

Jagran Institute of Management, Kanpur

MBA, MCA

Contact No : 0512- 2601126, 9336332150

Website : www.jimkanpur.ac.in • **Email :** adminjim@jef.org.in

Jagran Institute of Management and Mass Communication Kanpur and Noida

Advanced PG Diploma in Mass Communication, Print and Online Journalism, TV Journalism

Diploma in Mass Communication* with Bachelor Degree

Contact No: 8115927740, 8400791807 (Kanpur)

Website : www.jimmckanpur.ac.in, **Email:** jimmckanpur@rediffmail.com

8527473264, 8448952367 (Noida)

Website : www.jimmc.in • **Email:** directorjimmcn@jef.org.in

Jagran Institute of Digital Animation , Kanpur

3 Years Diploma in 3D Animation with Degree in Fine Arts

2 Years Diploma in Motion Graphics

1 Year Diploma in Graphics, Fine Arts, Fashion & Interior Designing

Contact No : 9839067435, 9919629846

Website : www.jidakanpur.com • **Email:** jida.director@gmail.com

Jagran School of Law , Dehradun

BA LL.B, BBA LL.B. , LL.B. , LL.M.

Contact No : 0135-2699992, 2699993

Website : www.jagranschooloflaw.com • **Email: info@jslddn.com**

Scholarships available for Meritorious Students

NATIONAL ACADEMIC DEPOSITORY

For details please visit : www.jef.org.in

JAGRAN JOURNAL OF MANAGEMENT AND TECHNOLOGY

• Volume 5 • August 2023

Registered with the Registrar of Newspapers of India Number UPENG/2019/78204

Printed & Published by
Dr. Anil Kumar Singh on behalf of Jagran Institute of Management

Publisher Address
Jagran Institute of Management
W-620, Juhi Saket Nagar, Kanpur (U.P.) - 208 014
Phone : 0512-2601126, 9336332150 • Follow us at:

Printed at
Solar Press
96/2, Chunniganj, Kanpur (U.P.) - 208 001

Email id : jjmtjim@jef.org.in • Website : www.jimkanpur.ac.in /jim-Journal-Portal.html

JAGRAN JOURNAL OF MANAGEMENT AND TECHNOLOGY

ANNUAL PEER REVIEWED JOURNAL OF JAGRAN INSTITUTE OF MANAGEMENT

The Jagran Journal of Management and Technology is a double-blind, peer-reviewed journal of Jagran Institute of Management. It carries theoretical and empirical papers, case studies, research notes and review articles, and aims at disseminating new knowledge in the field of different domain areas of management, information technology and related disciplines. The important role of providing a forum for exchange of knowledge among academics, industrialists, researchers, planners and the practitioners is executed by the Journal.

The aim of Jagran Journal of Management and Technology is to serve the profession by publishing significant scholarly research in management and information technology areas like business strategy, marketing, finance, human resource, retail , supply chain, international marketing, brand management, production and operations, environment management, entrepreneurship and SMEs, business intelligence and information system management, artificial intelligence, data base management, network security, data security, computer architecture, web application and services, software engineering and testing. The double blind peer review process adopted is aimed at enhancing the professional development of researchers.

EDITORIAL BOARD

Subscription Rates

The Subscription rates are as under :

Indian	Rs. 500/- Annual Subscription
Foreign	US $ 20 Annual Subscription

Additional shipping charges as applicable for destinations within or outside India.

Mode of Payment

Electronic Transfer/ Demand Draft /Cash
Credit: Jagran Institute of Management, Kanpur.
A/C No. 29640200000023
Bank: Bank of Baroda, Branch: Bara Bye Pass, Kanpur
RTGS/NEFT: IFSC Code: BARB0BARRAB (fifth character is “zero”)

All correspondence may be addressed to:

The Editor, Jagran Journal of Management and Technology , Jagran Institute of Management

INDEX

Normalization in Database Design: Minimizing Redundancy, Eliminating Anomalies, and Ensuring Data Integrity

[1]Dr. Anil Kumar Singh, Professor & Dean Jagran Institute of Management, Kanpur, Email: anil.sysadmin@gmail.com
[2]Mr. Anand Kumar Dixit, Assistant Professor, Jagran Institute of Management, Kanpur, Email: acheiveranand@gmail.com

Abstract:
This paper explores the crucial role of normalization in database design, focusing on its significance in minimizing redundancy, eliminating anomalies, and ensuring data integrity. It discusses the detrimental effects of redundancy, such as storage inefficiency and data inconsistencies, and highlights how normalization techniques address these challenges. Furthermore, the paper examines anomalies that arise during data manipulation operations and illustrates how normalization mitigates insertion, update, and deletion anomalies. By adhering to specific normal forms, such as First Normal Form (1NF), Second Normal Form (2NF), and Third Normal Form (3NF), normalization provides a framework for organizing data efficiently and maintaining data integrity. The paper concludes by emphasizing the benefits of normalization in improving database performance, reducing data redundancy, and facilitating effective data management.
Keywords: Normalization, Database Design, Redundancy, Anomalies, Data Integrity

Introduction

Normalization is the process of minimizing **redundancy** from a relation or set of relations [1],it is a fundamental concept in database design that aims to structure data in a logical and efficient manner. It involves a series of guidelines and principles that help organize and optimize the database's structure, leading to improved data integrity and reduced redundancy.
The primary objectives of normalization are as follows:

Minimize Redundancy: Redundancy refers to the duplication of data within a database [2]. It can waste storage space, introduce inconsistencies, and make data maintenance challenging. By applying normalization techniques, redundant data is eliminated or minimized, ensuring that each piece of information is stored in only one place. This optimization leads to efficient storage utilization and avoids data inconsistencies that can arise from redundant information.

Eliminate Anomalies: Anomalies occur when a database exhibits undesirable characteristics during data manipulation operations such as insertion, update, and deletion [3]. For example, an insertion anomaly could happen when trying to add a new record, but some required information is missing, preventing the record from being properly inserted. By normalizing the

database, these anomalies are minimized or eliminated, making data manipulation operations more reliable and consistent.

Divide and Link Tables: One of the central aspects of normalization involves dividing larger tables into smaller, more manageable tables. This process helps improve data organization and simplifies database management. The smaller tables can be linked together using relationships, which define how the tables are connected and allow for efficient data retrieval through join operations. By breaking down complex data into smaller entities, normalization facilitates better data understanding and enhances the overall database structure.

Apply Normal Forms: Normal forms are guidelines that provide criteria for structuring tables in a normalized manner. There are several normal forms, including the commonly used First Normal Form (1NF), Second Normal Form (2NF), and Third **Normal Form (3NF).** Each normal form has specific rules that aim to eliminate redundancy, ensure data dependencies are properly represented, and maintain data integrity. Applying these normal forms incrementally helps achieve a well-structured and normalized database design.

Normalization is a process that organizes database data, reduces redundancy, and eliminates anomalies. It involves dividing larger tables into smaller ones, linking them through relationships, and adhering to specific normal forms. By following normalization principles, databases can achieve improved data integrity, storage efficiency, and maintainability.

Row level Duplicacy: In the below table row 1 and row 3 are exactly same. It is known as row level duplicacy.

Student_id	Student_Name	Age
1	Saurabh	20
2	Aakash	21
1	Saurabh	20

Row level duplicacy can be removed with the help of Primary Key

Student_id (Primary Key)	Student_Name	Age
1	Saurabh	20
2	Aakash	21

Column level duplicacy

SID (Primary Key)	Sname	CID	CName	FID	Fname	Salary
1	Saurabh	C1	DBMS	F1	Adarsh	50000
2	Aakash	C2	C++	F2	Ashish	55000
3	Ravi	C1	DBMS	F1	Adarsh	50000
4	Nitin	C1	DBMS	F1	Adarsh	50000

In column CID and FID have duplicacy. It is known as column level duplicacy.
Due to the column level duplicacy three level problems such as insertion, deletion and updation arises which is known as anomalies, occurs on a special occasion.

Insert Anomalies: - Insert a student in above table (SID=5, Sname= Ajay). The student information will be easily inserted.

SID (Primary Key)	Sname	CID	CName	FID	Fname	Salary
1	Saurabh	C1	DBMS	F1	Adarsh	50000
2	Aakash	C2	C++	F2	Ashish	55000
3	Ravi	C1	DBMS	F1	Adarsh	50000
4	Nitin	C1	DBMS	F1	Adarsh	50000
5	Ajay	-	-	-	-	-

But we cannot insert the information of Course and Faculty. Because since the SID is a primary key, as per the property of primary key it cannot be NULL. What value you will put on SID.

Deletion Anomalies: - Delete the record which SID=1. You can easily delete without any negative impact on the table.
But when you delete the record which SID=2. It will also delete the information of Course ID= C2 and Faculty ID= F2

Updation Anomalies: - 1. Change the name of student form Nitin to Nitin Yadav which SID =4. It will easily update.

SID (Primary Key)	Sname	CID	CName	FID	Fname	Salary
1	Saurabh	C1	DBMS	F1	Adarsh	50000
2	Aakash	C2	C++	F2	Ashish	55000
3	Ravi	C1	DBMS	F1	Adarsh	50000
4	Nitin Yadav	C1	DBMS	F1	Adarsh	50000
5	Ajay	-	-	-	-	-

2. Update the salary of F1 from 50000 to 54000. It will update 50000 to 54000 where F1 will find. Since only one faculty whose FID=F1, therefore salary should be update only one time. But due to the column level duplicacy it updated many times.

Solution- Normalisation

The above anomalies such as insert, delete and update may be removed with help dividing above single table into following 3 tables.

Student

SID (Primary Key)	**Sname**
1	Saurabh
2	Aakash
3	Ravi
4	Nitin Yadav
5	Ajay

Course

CID (Primary Key)	**CName**
C1	DBMS
C2	C++
C1	DBMS
C1	DBMS

Faculty

FID (Primary Key)	**Fname**	**Salary**
F1	Adarsh	50000
F2	Ashish	55000

Normal Form

Roll No	Name	Course
1	Saurabh	C/C++
2	Aakash	JAVA
3	Ravi	C/DBMS

1NF – Table should not contain any multivalued attribute

1st Representation Table

Roll No	Name	Course
1	Saurabh	C
1	Saurabh	C++
2	Aakash	JAVA
3	Ravi	C
3	Ravi	DBMS

Primary Key (Composite Key) =Roll No + Course

2nd Representation of Table

Roll No	Name	Course1	Course2
1	Saurabh	C	C++
2	Aakash	JAVA	NULL
3	Ravi	C	DBMS

Primary Key= Roll No

3rd Representation of Table

Roll No (Primary Key)	Name
1	Saurabh
2	Aakash
3	Ravi

Roll No (Foreign Key)	Course (Primary Key)
1	C
1	C++
2	JAVA
3	C
3	DBMS

2nd Normal Form

Table or relation must be in 1st Normal Form and all the prime attributes should be fully functional dependent on candidate key.

CustomerID	StoreID	Location
1	1	Delhi
1	3	Mumbai
2	1	Delhi
3	2	Bangalore
4	3	Mumbai

Candidate key = CustomerID + StoreID
Prime attribute = (CustomerID, StoreID)
Non-Prime attribute (location)
In above table location is determined by the storeID. The table has partial dependency. Hence above table is not in 2nd Normal Form.
Now we will decompose above table into following tables.

CustomerID	StoreID
1	1
1	3
2	1
3	2
4	3

StoreID	Location
1	Delhi
3	Mumbai
1	Delhi
2	Bangalore
3	Mumbai

There should be no partial dependency in the relation.
Condition of partial dependency: - Any non-prime attribute determined by the part of the candidate key.

3rd Normal Form

Table or relation must be in 2nd Normal Form and there should be no transitive dependency in table.

RollNo	State	City
1	Punjab	
2	Haryana	
3	Punjab	
4	Haryana	
5	Bihar	

Transitive dependency: candidate key RollNo

RollNo--------→ State

Sate----------→ City

RollNo-------→City

For 3rd NF LHS must be candidate key or RHS must be prime attribute.

BCNF (Boyce Codd Normal Form) special case of third normal form. Table should be in third normal form. LHS must be a candidate key.

RollNo	**Name**	**Voter ID**	**Age**
1	Ravi	K0123	20
2	Varun	M034	21
3	Ravi	M786	23
4	Rahul	D286	21

Candidate Key (RollNo, VoterID)

FD(RollNo----→Name, RollNo-----→VoterID, VoterID--→Age, VoterID---→RollNo.

Conclusion

Normalization is a crucial process in database design that plays a vital role in minimizing redundancy, eliminating anomalies, and ensuring data integrity. By adhering to specific normal forms, such as First Normal Form (1NF), Second Normal Form (2NF), and Third Normal Form (3NF), database designers can create efficient and well-structured databases that optimize storage, improve data consistency, simplify maintenance, and support scalability. Throughout this paper, we have explored the significance of normalization in addressing various challenges in database design. We discussed the detrimental effects of redundancy, such as wasted storage space and data inconsistencies, and highlighted how normalization techniques help reduce redundancy by structuring data in a more organized and efficient manner.

Furthermore, we examined anomalies that can occur during data manipulation operations, including insertion, update, and deletion anomalies. These anomalies can compromise data integrity and lead to incorrect or inconsistent information. Through normalization, we can mitigate these anomalies by breaking down larger tables, establishing relationships, and ensuring that data dependencies are properly represented.

In conclusion, normalization is an essential technique in database design to minimize redundancy, eliminate anomalies, and ensure data integrity. By applying normalization principles, database designers can create efficient and reliable databases that effectively store and manage data. It is crucial for database practitioners to understand and implement normalization techniques to achieve optimal database performance and data consistency.

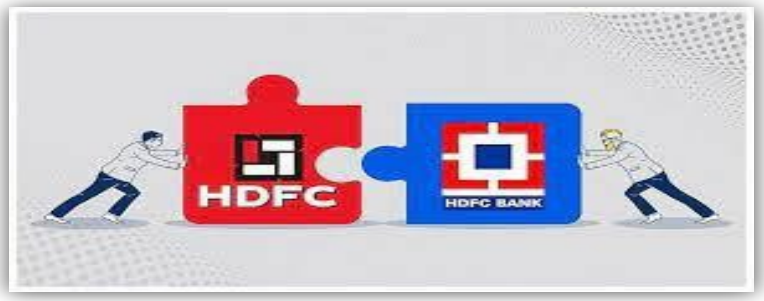
References

1. Normal Forms in DBMS, https://www.geeksforgeeks.org/normal-forms-in-dbms/
2. Alexander S. Gillis, Technical Writer and Editor, TechTarget," Redundant", https://www.techtarget.com/searchstorage/definition/redundant#:~:text=Data%20redundancy%20refers%20to%20the,data%20corruption%20or%20data%20loss.
3. VarmaSrikanth, DBMS Course - Master the Fundamentals and Advanced Concepts, https://www.scaler.com/topics/anomalies-in-dbms/

Mega Reverse Merger of HDFC Bank and HDFC Ltd: A Strategic Analysis and Implications

[1]Mr. Aryan Gupta, Student, MBA First Year, Jagran Institute of Management, aryangup.jim.mba.2022@gmail.com
[2]Mr. Pawan Omer, Assistant Professor, Jagran Institute of Management, pawan.omer@gmail.com

Abstract:-
This research paper aims to explore the potential strategic implications of a hypothetical mega reverse merger between HDFC Bank and HDFC Ltd, two leading financial institutions in India. The study investigates the rationale behind such a merger, analyzes the potential benefits and challenges, and examines the implications for various stakeholders, including shareholders, customers, employees, and regulators. Furthermore, the paper discusses the potential impact on the Indian banking and financial sector, as well as the broader economy. The research utilizes a combination of qualitative analysis and financial modeling to evaluate the feasibility and potential outcomes of this merger.When two separates' entities deal in same business industry and get merged it is called merger. In reverse merger case when a subsidiary company takes over the parent company it is called "It isjustlike a grown-up son acquiring father's business". Reverse Merger. Here itis to mention the quote by Deepak Parekh former Chairman of HDFC LTD.
Keywords: mega reverse, stakeholders,qualitative analysis,parent company



Introduction:-
The financial sector plays a crucial role in the economic growth and development of any country. In India, HDFC Bank and HDFC Ltd are two prominent financial institutions that have achieved significant success and established themselves as leaders in their respective domains. HDFC Bank is one of the largest private sector banks in India, offering a wide range of banking and financial services, while HDFC Ltd is a leading housing finance company providing housing loans and related services.

HDFC Bank as an acquiring company

HDFC Bank was started Jan 1995 after the RBI open the banking sector to private player. HDFC as a private bank who takes the deposit from public and lend money to earn some interest as a profit. HDFC is one of the leading private banks in India who has low debt as well as low NPA (Non - Performing Assets) with better service and high market share in India. HDFC also involve with neo banking (inter
-connection system of online banking transactions) to give his customers high quality service.

ResearchObjectives:–

The primary objective of this research paper is to analyze the potential implications and strategic considerations of a hypothetical mega reverse merger between HDFC Bank and HDFC Ltd. The study aims to explore the motivations behind such a merger, evaluate the potential benefits and challenges, and assess the impact on various stakeholders. Additionally, the research seeks to examine the broader implications for the Indian banking and financial sector.

1- Rationale Analysis: Investigate the strategic motivations behind a mega reverse merger between HDFC Bank and HDFC Ltd.
2- Benefits and Challenges Assessment: Evaluate the potential benefits and challenges of the merger for various stakeholders, including shareholders, customers, employees, and regulators.
3- Financial Analysis and Projections: Conduct a comprehensive financial analysis of the consolidated entity resulting from the merger. Assess the potential financial performance, profitability, liquidity, and solvency of the merged organization
4- Stakeholder Perspectives: Understand the perspectives of various stakeholders, including shareholders, customers, employees, and regulators, regarding the proposed mega reverse merger.
5- Managerial and Policy Recommendations: Based on the analysis of the strategic implications and stakeholder perspectives, provide recommendations for managers, policymakers, and regulators involved in the decision-making process.

By addressing these research objectives, this study aims to contribute to the existing knowledge and understanding of mergers and acquisitions in the financial sector, specifically focusing on the strategic implications of a mega reverse merger between HDFC Bank and HDFC Ltd.

Key Functions of HDFC Bank:-

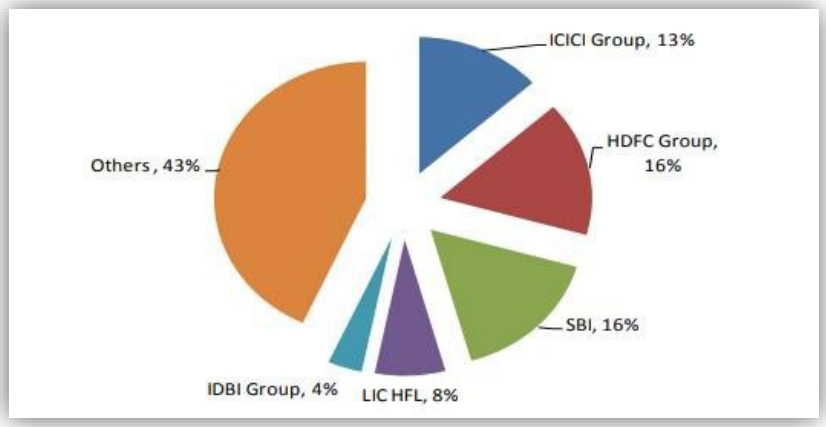
To know about HDFC Bank in depth here some important functions of HDFC Bank are mentioned below.

- In India HDFC Bank deals in deposit money and lendingfacility.

- HDFC Bank also provide the fixed depositfacility.
- HDFC Bank provide the whole sale bankingfacility.
- HDFC Bank sell their products like - credit cards , debit cards , lifestyle loans etc.
- HDFC Bank also deals in treasury services like Debt capital markets , Equities Research - Reports & commentary on markets and currencies, Asset liability management , foreign exchange &derivative.

HDFC LTD as a target company

HDFC LTD was set up by **HasmukhLalThakor das Parekh** uncle of **Deepak Parekh former Chairman of HDFC LTD** in 1977. HDFC LTDis NBFC who lends only for housing loans and makes profit. HDFC LTDis leading housing loan provider in India. inIndia. It covers total 16% of market share by GDFC Group in housing loans. In India HDFC LTD is one of the most sustainable NBFC corporation who tackle the all-financial crisis veryefficiently.



Source- The economic Times

Key functions of HDFC LTD–

As a leading NBFC and jousting loan provider HDFC LTD also have some different type of products and services. Here somefunctions are mentionedbelow.

- HDFC LTD deals in mortgage business like home loans, construction of a residential units, purchase of land, home extension loans, non-residential premise loansetc.
- HDFC LTD gives the insurance productsfacility.
- HDFC LTD deals in general insurance motor, health, travel, home, and personal accident in the retailsegment.

Why this merger is required?

According to company report and various external study we have some important highlights are mentioned here but before that let quick understand what company management think on this merger HDFC Bank has a strong presence in urban and semi-urban areas, while HDFC Ltd has a wider reach across both urban and rural markets. The merger allows for geographic expansion, enabling the combined entity to tap into previously untapped markets and cater to a more diverse customerbase.

- When this merger is announcing Apr 2022 that time repo rate was 4% and now current repo rate is 6.50% same as CRR and SLR ration is also very low to maintain but the positive factor is to maintain these ratio HDFCLTD has good cash reserve so they want to use their resources at better place for the growth of theindustry.
- Additional factor is HDFC LTD leadership was closing 70 so that is also the part to merge both entity and give new leader to thiscompany.
- Merge both the companies to tackle with new NBFC players and reduce the cost.
- Make housing loans more competitive and fight with the other giants like – LIC, SBI,and PNBHousing Loansetc.
- Last and very important reason of this merger both entities have physical presence on various city so after this merger when HDFC LTD idmergedwith HDFC Bank then the rental and excessive man power is going to be less and make moreprofit

How big this merger is?

This merger is complete with $40 Billion somewhere around 3280 Cr. Where HDFCBank is acquiring to the HDFC LTD. HDFC Bank & HDFC LTDnow
creating the history because this merger is one of the biggest banking mergers and
after this merger HDFC Bank is one of the leading banks according to market capitalization which is around 14 lacksCr.

1 HDFC Bank (post-merger) 14,12,055.5

2 ICICI Bank Ltd 6,53,704.04

3 State Bank of India 5,11,201.77

4 Kotak Mahindra Bank Ltd 3,66,967.55

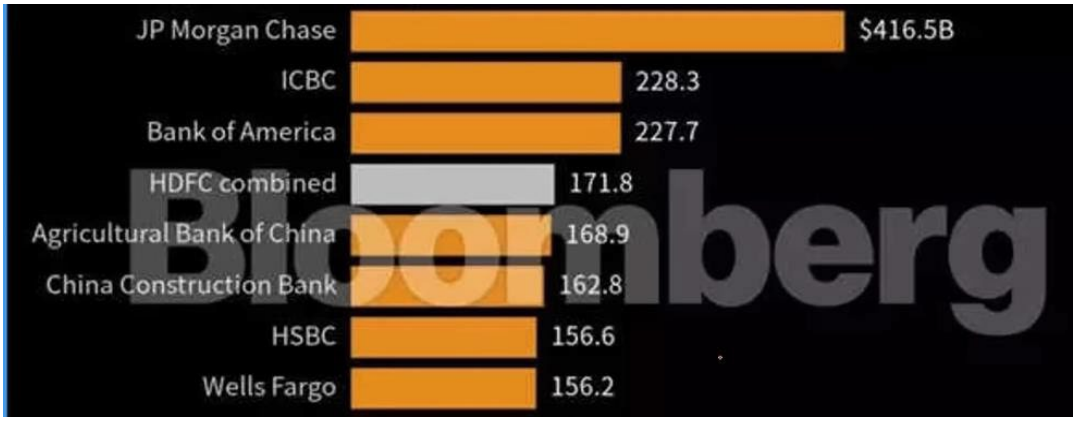
5 Axis Bank Ltd 3,04,211.88

6 Indusind Bank Ltd 1,06,707.03

Company thought on this merger **KekiMistry CEO of HDFC LTD** said "adding that the move will improve the bank's mortgage portfolio and attract more customers with a range of financialservices."

Impact of this merger on global level

According to Bloomberg report this merger stand out the HDFC Bank in top 5 financial services at global level with $171.8BillionPost merger HDFC Bank is standing on top 5 financial institutions with big giant like J.P Morgan , ICBC , Bank of America before merger globally this listisdominated by the American.



Source:-www. Bloomberg.com

Impact of this merger in India

Here some important key highlights of this merger and the impact in India are mentioned–

- After merger HDFC Bank is leading bank in India with 14 Lack Cr. market capitalization. The merger ratio is 25:42 means HDFC Bank will give 42 shares to HDFC LTD shareholders for every own of 25 shares of HDFCLTD.
- HDFC-HDFC Bank merger will be effective on July 1. The boards of HDFC and the private bank will meet on June 30 post to clear and approve the merger.
- On Indian Stock Exchange both HDFC entity will stop trading on the stock exchange on 13 July and the merged entity is expected to be back for trading by 17July.

Working function of the HDFC Bank post-merger

- Your FD Account Number continues to be the same and will remain the reference point for all your future communications with HDFCBank
- Yourexisting Deposit issued by HDFC Limited will continue to be valid till the

maturity of theFD

- Recurring Deposits : Your existing recurring deposit will continue and monthly installments will be debited from the linked account as updated against the RD as per the mandatesubmitted.
- The existing threshold limit for TDS deduction is ₹5,000 for the customers of HDFC Limited. After the merger threshold limit of ₹5,000 will changeto
  ₹40,000 (₹50,000 for senior citizens) for all the existing customers of HDFC Limited.

Conclusion:-

This research paper provides an in-depth analysis of a hypothetical mega reverse merger between HDFC Bank and HDFC Ltd. It examines the strategic rationale, potential benefits, and challenges associated with the merger. The study also evaluates the financial implications and projections, along with the broader impact on stakeholders and the banking sector. The findings of this research will contribute to a better understanding of the potential implications of such a significant merger in the Indian financial industry.

References:-

1- https://csuglobal.edu/blog/why-ai-important
2- https://csuglobal.edu/blog/why-ai-important
3- International Development Research Centre,(1996) ,available in the internet http://www.fao.org/docrep/w6840e/w6840e02.html
4- https://www.5paisa.com/news/hdfc-to-merge-into-hdfc-bank
5- http://www.bloombergquint.com/

Cyber Security: The Significant Role and Impact of Artificial Intelligence, Machine Learning and Data Mining

Mr. Vishnu Kumar Shukla, (Assistant Professor, Department of MCA), Jagran Institute of Management, Kanpur (UP), India, (Dr. A.P.J. Abdul Kalam Technical University, Luck now), Email: vishnu10sh@gmail.com

Abstract: The fast development of information technology has encouraged many organizations to depend on internet connections for sensitive business data operations every day. These networks have become more vulnerable than ever to cyber security attacks and risk.
Today, the ransomware and cyber-attack are changing the scenarios for the IT sector. The ransomware threat is a top issue for many organizations. Few organizations are totally prepared for an attack or its backup recovery but backup recovery only is not enough. It's important to stop ransomware in its tracks with a set of integrated capabilities. Stopping cyber-criminals is the key in this game. There are many benefits from the use of new technology, on the other hand cyber attack have created many problem for organization and individuals. Therefore, organizations need to redefine how to strengthen their infrastructure, protect their valuable data assets and reduce business risk. Organizations, individual and IT professionals must stay one step ahead and invest in proactive technology that improves their organization's cyber-resilience. The combination of data security and cyber security is a new experiment of every organization.

According to general report of Cybercrime Magazine, the total cost of global cybercrime is expected to reach $8 trillion by the end of during period of 2023. This cost is predicted to incremental grow by 15% every year, reaching $10.5 trillion by during period of 2025. So no doubt the cyber-attack or cyber-threats in the modern world is massive and continues to exponentially grow very fast. Therefore, arise a big question, how to safeguard our online digital world.

In an ever-evolving digital space full of cyber threats, the combination of Artificial Intelligence, Machine Learning and Data Mining is changing the way of digital space where we protect our online cyberspace. With the ability to intelligently simulate human behavior and analyze large set of data. Therefore Artificial Intelligence (AI) Machine Learning and Data Mining play a very important role in generating, monitoring and controlling cyber attack intelligence to beat against cybercrime in term of cyber security.

In this paper, we describe the various profound significant roles and impact of artificial intelligence, machine learning and data mining in the realm of Cyber Security can generate

robust models for malware & intrusion detection and execution of malware classification for the promising future they required. Organizations and Individuals can powerful their security by harnessing the strength of Artificial Intelligence (AI), Machine Learning (ML) and Data Mining (DM) to proactively defend against malicious threats on their networks and reduce their cyber risks.

Keyword: Artificial Intelligence, Machine Learning, Data Mining, Cyber Security, AI, ML, Cyber Attack, ransomware, algorithm, technique, malware, intrusion, fraudulent, threat intelligence, bots, smart bots, web crawlers, classification, clustering, zero-day attack, regression, time series etc.

1. Introduction: Information Technology is changing rapidly. No doubt we have a number of benefits of digital land space but it also has its issues and challenges as well. Artificial Intelligence is increasing every day by day. AI technology was first introduced to the market and the quick change in technology and business industries. Computer scientists are expecting that AI market by 2025, "85% of users interactions will be managed without a human". AI application has grown to be very popular in today and greatly apply the significant impacts the quality of lives we live.

Machine learning is the also part of artificial intelligence that support in building the systems that can learn or train based on previous experience and perform different actions based on historical data (Donepudi, 2019). A number of machine learning algorithms are available that covered the supervised, unsupervised, reinforcement machine learning algorithms. These algorithms first have to be collect data and train the data known as train data set. After train the data set training, these algorithms can be used to perform multiple tasks in various sectors. In mostly, machine learning algorithms are used for prediction purpose and to detect something that is hidden or visual.

Figure: Cyber Security

Online platforms are helpful for the organizations and individuals because they can easily access own data. But the problem is this gives the opportunity to the cyber criminals to hack the data or personal information via online platforms. This type of activity can be proved harmful to an individual, organization and society. Stopping the cyber crime is a very big challenge because it is not an easy task.

The use of artificial intelligence, machine learning and data mining algorithms and is proving helpful in cyber security risk and issues. IT professional are using different algorithms to solve the cyber security issues and risk using creating a strong firewall for cyber space (web space). The algorithms of machine learning and data mining with the help of artificial intelligence are trained to profound the cyber attacker and fulfill the purpose of organizations and individuals. These algorithms will detect the cyber attacker automatically once they have trained.

Only in 2022, humans created, copied and consumed around 90ZB (zetta-bytes) of data. It may seem look like we have all the data we need, its duty of every organization provides the safe guard for data. Data Mining provides a safe guard for your data and it to improve our cyber security firewall. Data Mining technique can help you improve the detection of malware, network and system intrusions, insider attacks and many other security threats based on analyzing your databases and security logs. Some techniques of data mining can accurately predict attacks and detect zero-day threats.

2. Artificial Intelligence: Artificial Intelligence was first invented by Scientist John McCarthy in 1956 in conference. The idea of machines operating like human beings started to be the scientist's mind and whether if it is possible to build computers has the same ability to think and learn by itself and give the name by the mathematician Alan Turing. Alan Turing was capable to put his hypotheses theorem and questions into actions by testing result i.e. "machines can think", after series of test called as Turing Test machine. It turns out that it is possible to enable machines to think and learn just like humans being. Turing Test machine is able to identify if machines can respond as humans being.

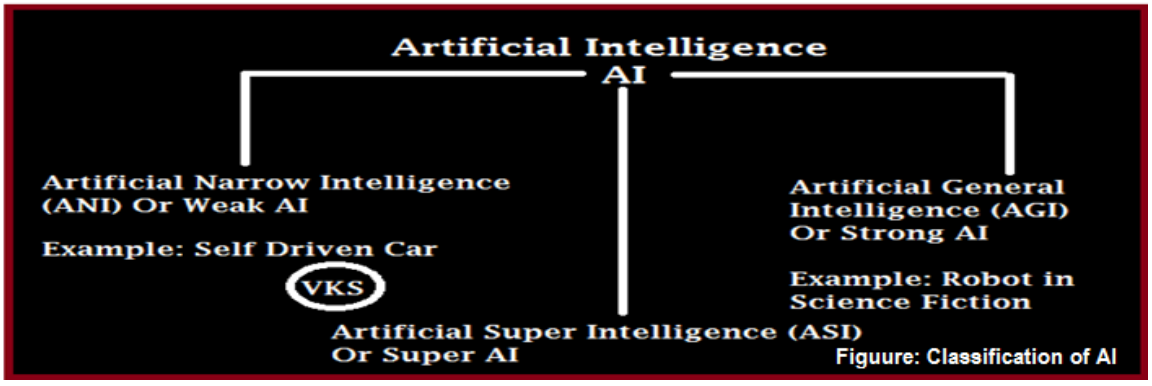
2.1 Definition: Artificial intelligence is a field of computer science that offers machines to learn from experience and perform tasks that usually need human intelligence. The objective of this technology is to enhance human capabilities and contributions not replace them. AI makes it a valuable organization and individual asset.

In traditional IT System, artificial intelligence (AI) is simply methodology that enables machines train, develop and demonstrate same as a human behavior. Artificial intelligence (AI) systems includes process such as learning, planning, reasoning, decision making and problem-solving carrying out group of tasks and solve problem same as humans intelligence do. In business world, we are refer in three category of Artificial Intelligence (AI)-

2.1.1. Artificial Narrow Intelligence/Weak Artificial Intelligence: This classification of **Artificial Intelligence** (AI) refers to Internet on Things (IoT) based product can only do things they are trained to do.

2.1.2. Artificial General Intelligence/ Strong Artificial Intelligence: This classification of **Artificial Intelligence** (AI) refers to only to understand in science-fiction films, where machines can generalize between multiple tasks just like humans do. Think of such movies are Robot (2004), Chappie (2015) etc.

2.1.3. Artificial Super Intelligence/Super Artificial Intelligence: This classification of **Artificial Intelligence)** (AI) refers with strong capabilities than human's intelligence; say that, this type is way far from realization as a visual.



Figuure: Classification of AI

3. Artificial Intelligence Tools for Cyber Security: There are various common tools available are frequently used in cyber security for any organization:

3.1 Sophos Intercept X tool: This is very popular tools for software and hardware security and invented by British company. Sophos intercept X tool is an excellent to finding malware defense solution for organizations and individuals. This tool uses a deep learning neural network algorithm that mimics a human intelligence to access millions of features from a data file and perform an in-depth analysis and justify determining whether it is harmful, benevolent or not.

3.2 Vectra's Cognito: This tool is real time malware detective tools based on AI algorithm. It is very frequently used data gathering from cloud events and network usage data and also uses behavioral detection algorithms to unmask hidden attackers in IoT (Internet on Things) devices.

3.3 Darktrace Antigena: This tool is also real time self-defense product detective tools that recognizes and reacts to malicious behavior in real-time. It takes targeted action to neutralize attacks on emails, protecting employees, organization data file from threats, malware and spear phishing.

4. Machine Learning: Machine learning is also part of science which was found as a subfield of artificial intelligence and developed in the around 1950s. But, In 1990s, the researcher's start on this field restarted, developed and has reached to today that will improve more in the future. The main thing of this development is the difficulty of analyzing and processing the increasing data every day. Machine learning is based on the principle of finding the best model for the analyzing and processing new data among the previous data. In machine learning, there is no error gap in the operations carried out by machine based an algorithm i.e. machine learning is the way of joining the machine with the ability to learn by using the data and experience like a human intelligence.

4.1 Definition: Machine learning is a set of techniques, methods and algorithms used to train machines to process, analyze and find hidden solution patterns in data and make decision making solution. Machine Learning technology or algorithm is to utilize data for self-learning & eliminating the need to machine in put an explicit order. The main objective of machine learning is to generate models which can train themselves to improve, perceive the complex patterns and provide solutions to the new data or problems by using the previous problem or data .Machine once trained on data, machines can generate memorized patterns on new data and make better solution for decision making for future predictions.

Machine learning has many technical view, we are refer in four view of Machine learning (ML)-
4.1.1 Supervised Learning Machines: Machines are trained to discover solutions to a given problem with help of human-intelligence, who collect and process (label) data and then feed it to machine, and it can observe patterns, put objects with corresponding classes and evaluate whether their prediction is wrong or right.

4.1.2 Unsupervised Learning Machines: Machines are learning to identify hidden patterns and put (trends) in unlabeled training data without being supervised by users.

4.1.3 Semi-supervised Learning Machines: Machines are learn or trained with a dataset of labeled data and a huge amount of unlabeled data making of supervised learning and unsupervised learning.

4.1.4 In reinforcement Learning Machines: Machine are learn or trained to discover an optimal solution put in a closed unfamiliar environment to them, and must discover a solution to a problem by going through serial trials and errors. So machines get a reward for successful trial and receive punishment for find an error.

5. Data Mining: Data mining is the way of arrangement of huge amount of dataset to find anomalies identify patterns and relationships that can be managed to solve complex or business related issues. It can be used by individual and organizations for fraud detection and filtering to interest about customer. Therefore data mining is very important in terms of cyber security.

5.1 Data Mining Process in Cyber Security: Data mining is the way of analyzing data, discovering new patterns for data and predicting future trends for particular problem. It's specially used in scientific research industry, business development industry, customer relations service sector and other spheres. In another term of data mining is specially treated for knowledge discovery in databases (KDD). The main objective of knowledge discovery in databases (KDD) is to extracting useful and often previously unknown information from huge amount of dataset. The following figure of knowledge discovery in databases (KDD) process covered four steps:

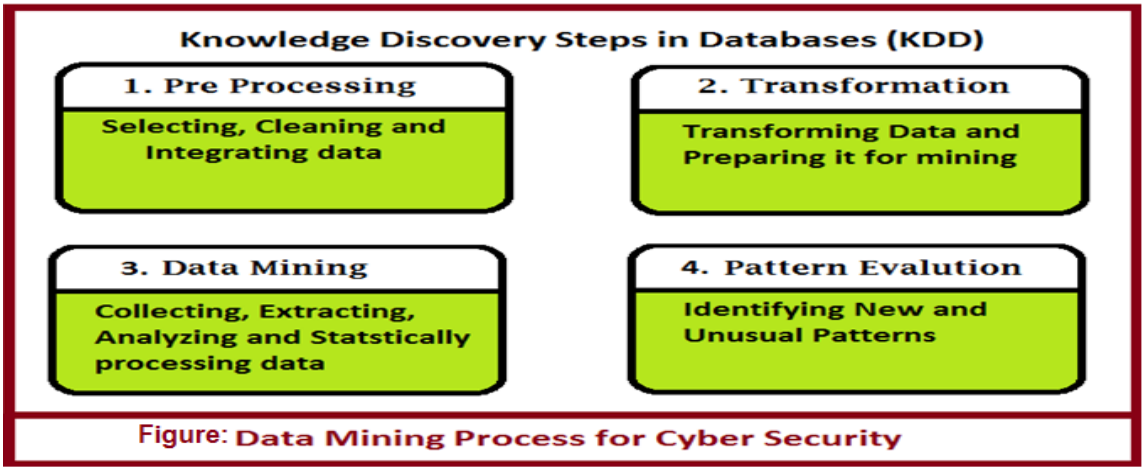


Figure: Data Mining Process for Cyber Security

Access the valuable knowledge in data mining uses various techniques from artificial intelligence machine learning, statistics and database systems. The process steps of data mining are two parts that are called data pre-processing and actual data mining.

The first one include steps such as data cleansing, data integration and data transformation while actual data mining is pattern assessment and knowledge representation of data in an understandable form. Data mining is often seen as a part of a richer field called Knowledge Discovery in Databases (KDD).

6. Artificial Intelligence and Data Mining Techniques/Tools for Cyber Security: Data mining uses various techniques and algorithms to turn huge volumes of data into useful information. There are various techniques available are frequently used in cyber security:

There are two types of model used in data mining based on **predictive or descriptive techniques**. Predictive techniques make predictions based on past events; but descriptive techniques are based on the analysis and structuring of existing data in database. There are six data mining techniques based on Predictive and descriptive techniques in for cyber security:

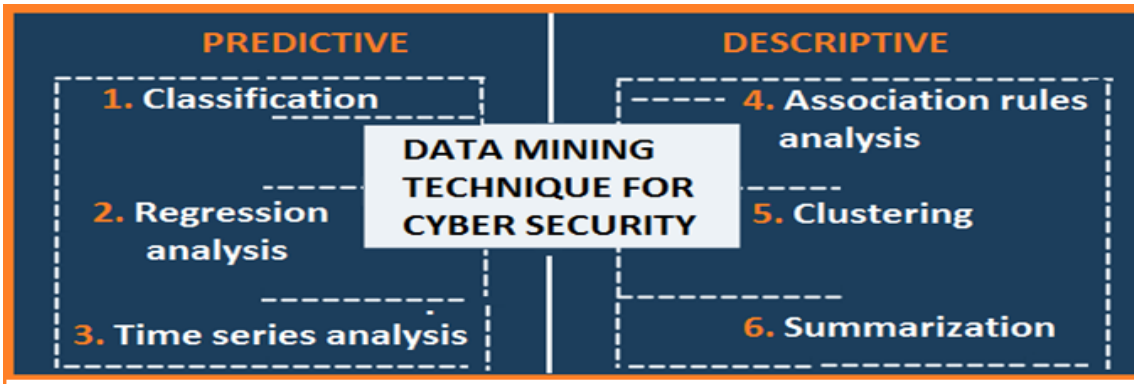


Figure: Data Miming Algorithms/Techniques

I. Classification Technique/Model: The classification technique creates a base model of your database by split a huge amount of dataset into predefined classes, methods and groups of variables. It is also useful to analyze variables with the database after create the model and include them with an appropriate class and group. To get accurate real-time classification, organization and individual to spent a lot of time to supervised training of the algorithm as well as to testing how it works on between their function. In cyber security, classification model is frequently used to find or detect spam and phishing emails.

II. Regression Analysis Algorithm/Technique: These technique or algorithms predict the convert value of one variable based on the previous or known average values of other variables in a dataset. Organization and individuals can make a relationship technique between dependent and independent variables in the dataset in database. This algorithm also gives the clarification of analyzing changes in variables and comparing these changes to the dependent variables. This technique is broadly used for forecasting trends or events for possible cyber attacks.

III. Time Series Algorithm/Technique: Time series algorithms identified and predict time-based patterns by analyzing the time of any event changes in the dataset in database. This algorithm is useful for getting all sorts of periodic schedule activities by mining multi-year dataset in databases. Organization and individual's works on rely on time series analysis for predicting security vulnerabilities and attacks finding the solutions that occur during a certain event, season and even time of the day & date.

IV. Association Rules Analysis Algorithm: This algorithm is one of the most used a groups of data mining. With the help of association rules analysis, organization and individual find possible relationship between variables that appear together in database and also find or discover hidden patterns in dataset. This technique is used to analyze and predict user behavior or intelligence, examine network traffic and define patterns of cyber attacks.

V. Clustering Algorithm/Model: Clustering This Algorithm helps organization and individual to identify data items that have common characteristics behavior i.e. understand to similarities and differences in variables. Many features of this technique, Similar to classification Algorithm but this algorithm cannot sort variables in real time. Clustering algorithm allows for making changes in the model and creating sub-clusters without having to reuse or rework all the algorithms.

VI. Summarization Technique/Model: Summarization technique is totally devoted or focused for summarization of dataset i.e. compiling brief descriptions of datasets, classes, variable and clusters. Summarization technique can help organization and individual better understand the contents or data item of your datasets and the output or result of the data mining process by grasping the essence of data and eliminating the need to dig through it manually. Summarization technique is mostly used in cyber security to generate reports and visualize logs table.

The above data mining techniques is very frequently used with Artificial Intelligence (AI) and Machine Learning (ML) algorithms.

7. Artificial Intelligence and Data Mining Application uses in Cyber Security: Data mining and AI algorithms are frequently useful to discover unusual data records or hidden pattern and events that may indicate a security issues in cyber world. There are the most common applications of data mining used in computer security:

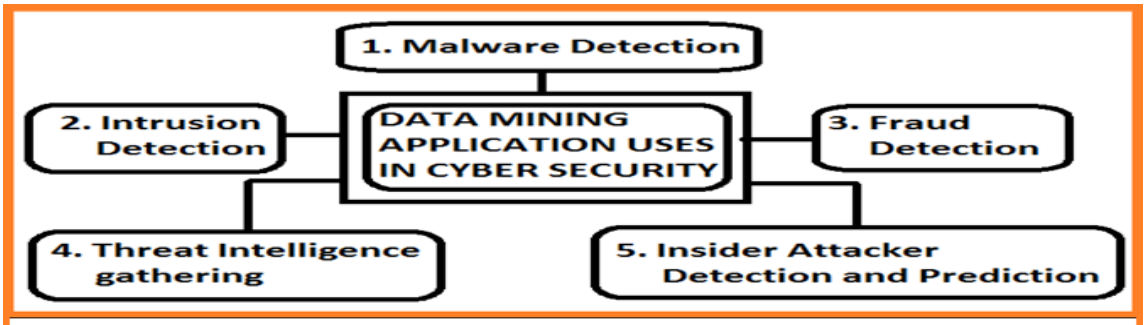


Figure: Classification of Artificial Intelligence and Data Mining Application uses in Cyber Security

1. Malware detection: Organization and Individual creating a security software, they use data mining technique to improve the speed and quality of malware detection technique with detect zero-day attacks. There are various strategies for finding or detecting malware:

I. Anomaly Detection includes modeling the normal behavior of a machine and network in order to identify deviations from normal activity patterns. This technique can detect even previously unknown attacks and can be used for defining signatures for misuse detectors.

Anomaly detection technique generates a report even legitimate event if it deviates from the normal behavior thus producing false positive alerts occurred.

II. Misuse Detection technique identifies only known attacks based on examples of their signatures; it is also known as signature-based detection technique. This technique has a lower rate of false positives and cannot work on detect zero-day attacks technique.

III. Hybrid Detection is combination of anomaly detection technique and misuse detection techniques in order to increase the number of intrusions detection while decreasing the number of false positives.

Malware Detection Process: Don't worry, which technique you select always follow the development of malware detection. Malware detection software has two steps process:

I). Extracting Malware Feature: The data mining algorithm extracts malware function from records on API calls, binary strings, program behaviors, N-grams etc. Developers can apply static, dynamic or hybrid analysis to extract malware function from unsafe files.

II). Classifying and Clustering: Selecting classification and clustering algorithm, use corresponding techniques to divide file into groups based on analysis and make a classifier using classification algorithms such as DECISION TREE, ARTIFICIAL NEURAL NETWORK, RIPPER, NAÏVE-BAYES AND SUPPORT VECTOR MACHINES (SVM). Each classification and clustering algorithm makes a model that represents both benign and malicious classes using machine learning (ML).

2. Intrusion Detection: Cyber Hacker can run malicious intrusions program via an organization's networks, databases, servers, web clients and operating systems. Using data mining techniques, organization and individual analyze and filtering audit results and identifies hidden or anomalous pattern. After scanning, organization and individual discover and detect intrusions, malicious code, network & system, denial of service (DoS) and penetration attacks. Data mining and AI algorithm or techniques are especially effective to find or detect two types of intrusions or threats:

I. Host-Based Attacks: This type of attack, Cyber security software needs to analyze and identified behavior and features extracted from programs. Occasionally this type of attack occurs particular machine or on a group of machines. In Host based system, Intrusion detection technique implements on customer hardware. In cloud, intrusion detection system (IDS) implement protects and secures data in cloud deployments.

II. Network-Based Attacks: This type of attack occurs when the attack on the network then your cyber security software needs to find a solution to analyze entire network traffic.

Intrusion detection technique is usually based on classification algorithm, clustering algorithm, and association rules algorithm. Intrusion detection techniques allow for extracting attack features from a database, systemizing them and alert or flagging any new records or dataset with the same features. There are some of the algorithms for intrusion detection such as REGRESSION ANALYSIS, DECISION TREES, BAYESIAN NETWORKS, K-NEAREST NEIGHBORS and HIERARCHICAL CLUSTERING etc. Organization and Individual can also use for future prediction capabilities to the intrusion detection system like classification and time series analysis algorithm. Artificial Intelligence (AI) algorithms will make it easier to detect hidden or previously unknown suspicious activity.

3. Fraud Detection: The detecting of fraudulent is challenging task because fraudulent activities are usually well-hidden and cybercriminals constantly change new fraud patterns. Data mining and artificial intelligence algorithm that allow machine learning can hold many types of fraudulent from financial to telecommunications fraud and system intrusions. Machine Learning is especially useful for fraud detection because it can: 1. Record maintain to take into account changes in the number and complexity of your databases. 2. Learn and trained to detect and predict new kind of fraud. 3. Analyzing and calculating the probability of fraudulent activity. Support to machine learning supervised and unsupervised algorithms to detect or find fraudulent type activity.

A. Supervised Learning: All available records are classified with the help of classification algorithm as either fraudulent or non-fraudulent. The classification algorithm is use for training a model to detect possible fraudulent. The main drawback of this algorithm, it is not able to detect new kind of fraudulent or attack.

B. Un-Supervised Learning: This algorithm to learn fraudulent patterns from untagged dataset or records. They make their own classification and feature descriptions for fraudulent activities. This algorithm also helps to identify privacy and security issues in dataset without using statistical analysis. It is also capable of analyzing and detecting new kind of fraudulent.

4. Threat Intelligence Gathering: Data mining algorithms support to find and discover hidden type data and change it into a structured threat intelligence dataset, after that a cyber security expert has to manually review discovered data and take a decision how to act on it. There are some of algorithm such as Clustering, Association Rules and Summarization algorithm to finding or discover these types of threat intelligence. However, Organization and individual can also add data mining techniques to make a machine learning (ML)-based framework for collecting and processing data in cyber security. The main issue is to find a relevant piece of data in terabytes (TB) of records.

5. Internal Threat Detection: Internal threats (attacker) are activities of legitimate users that may cause harm to an own organization. The detecting of internal threat activities is usually a

shorten task, because these actions often look same to ordinary user activities or they can be purposely masked from threat detection technique. So big data algorithms can detect unusual behavior of both machine and human-being are widely used to detect and predict insider threats. Similar to intrusion detection systems, internal threat detection (ITD) systems are based on identifying features of legitimate and threatening actions. There is a great achievement of machine learning-based classification & clustering algorithms for supervised and unsupervised that help to detect internal (insider) threats. Also use of deep neural networks based on data mining principles to examine cyber security user's logs and detect possible internal activity in real time.

8. Smart Bots in Cyber Security under Artificial Intelligence Machine Learning and Data Mining: Overview: Today, a huge amount of data traffic in internet to force for making a smart bots. Bots are basically software that performs automated job, pre-defined, and repetitive tasks much faster than human being do. There are some name of bots includes:

I. Chat Bots: These are bots that able to conversation same as human being. They give respond to certain phrases or sentence with programmed instruction replies.

II. Social Bots: Social bots that operate on social media platforms. I.e. face book, twitter, product and customer support related chat boat etc.

III. Web Crawlers: Web crawlers are sometimes known as spider bots. It access through web browsers via the web pages on the internet with the objective of web indexing.

IV. Malicious Bots: These bots are useful are programmed to gain unauthorized access to user accounts and perform other unethical or cyber-crime to include these attacks, malicious code is known as malicious bot is distributed in a botnet i.e. similar files or copies of the bot are distributed across multiple machines or devices normally without the knowledge of the owners. If the machines are located in different IP (Internet Addressed) addresses, it's hard to discover or identify and block the source of the malicious data.

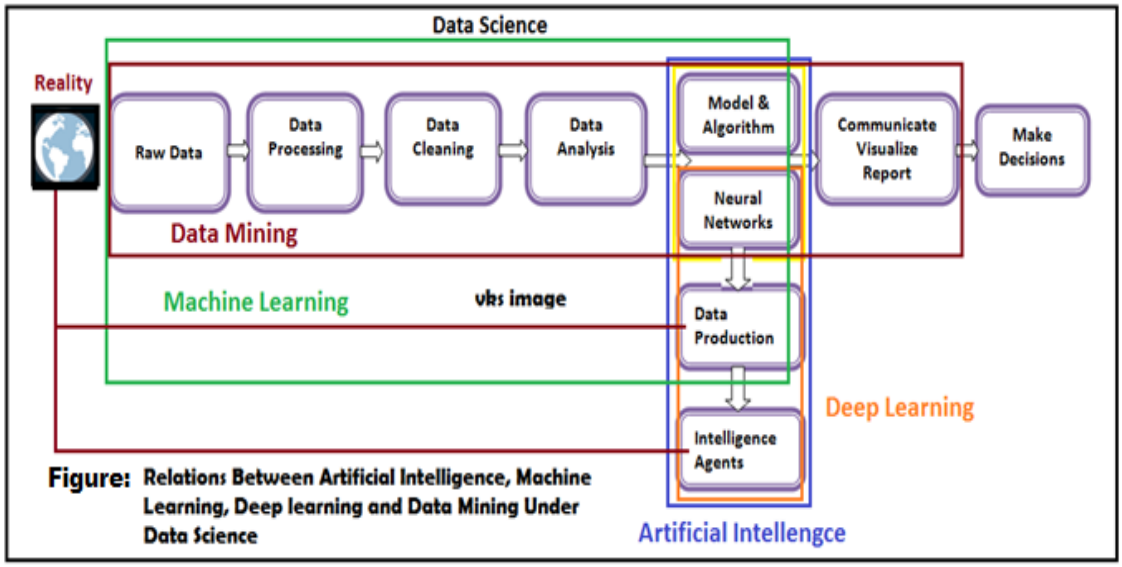


Figure: Relations Between Artificial Intelligence, Machine Learning, Deep learning and Data Mining Under Data Science

This type of problems is very easy to find solution through artificial intelligence and data mining in cyber security and also easier to understand of the web traffic and differentiate between bad and good bots. Example-signatures, if a malware signature is specified in an object then that object are regarded as malicious.

Conclusion: In this paper, the above Artificial Intelligence (AI), Machine Learning (ML) algorithms and Data Mining techniques is very useful to discover more hidden pattern and also improve the accuracy of security and prediction of future cyber attack in cyber world. These technologies are discover to a cyber security solution and will surely add to the complexity of its development and maintenance. The intensity of cybercrime attackers continue to evolve rapidly with each passing year. However, these technologies in cyber security are providing fast-emerging trends that enhance the performance of IT security World. They give the much-needed threat identification and analysis and security issues can possible to minimize breaches and strengthen security structure and posture.

Every user wants to access safe, secure, reliable, relevant and well-structured data, while organizations generate tons of data every day, manually gathering and processing all that data to combat cyber security threats is impossible, so these technologies can support you identify the behavior, characteristics and features of any malicious activity and predict the possible attacks by cyber attackers. They are particularly work on gathering threat intelligence and detecting malware, intrusions, fraudulent and insider attacks. To enhancing your protection with these technologies is the ability to identify zero-day attacks.

References: -

[01] Sumeet Dua, Xian Du. "Data Mining and Machine Learning in Cyber security". New York: Auerbach Publications. 19 April 2016.

[02] RAY, S. https://www.analyticsvidhya.com/blog/2017/09/common-machine-learning-algorithms/ 2017, September

[03] https://cybersecurityventures.com/

[04] Sarker IH. Machine learning: Algorithms, real-world applications and research directions. SN computer. Science. 2021; 2(3):1–21.

[05] https://www.apriorit.com/

[06] https://addepto.com/

[07] S. Sumathi, S.N. Sivanandam- Data Mining and its Applications

[08] https://read.commvault.com/deceiving-ransomware-with-commvault-esg-infographic?

[09] Kaelbling LP, Littman ML, Moore AW. Reinforcement learning:

[11] A survey. J Artif Intell Res. 1996; 4:237–85. [10] Xin Y, Kong L, Liu Z, Chen Y, Li Y, Zhu H, Gao M, Hou H,Wang C. Machine learning and deep learning methods for cyber security Ieee access. 2018; 6:35365–81.

[12] Neeraj Bhargava, Ritu Bhargava, Pramod Singh Rathore, and Rashmi Agrawal Artificial Intelligence And Data Mining In Security Frameworks

[13] Data Mining and Machine Learning in Cyber security By Sumeet Dua, Xian Du Data Mining for Intelligence, Fraud & Criminal Detection Advanced Analytics & Information Sharing Technologies by Christopher Westphal

[14]https://www.researchgate.net/publication/346703112_Automation_and_Machine_Learning_in_Transforming_the_Financial_Industry

Work-Life Balance of Women Employees

[1]Himanshi Tiwari, Student, Jagran institute of Management, himineeraj26@gmail.com
[2]Ms Priya chopra Arora, Assistant Professor,Jagran Institute of Management, chopra.priya63@gmail.com

ABSTRACT

Work-life balance is a term used to describe the balance between an individual's professional and personal life. A healthy work-life balance assumes great significance for working women particularly in the current context in which both, the family and the workplace have posed several challenges and problems for women. In this literature review, the study has revealed that women usually face role conflict more than men. Work-family conflict occurs when an individual experiences incompatible demands between family and work roles, causing participation in both roles to become more difficult. This imbalance creates conflict at the work-life interface. Many family-friendly organizations feel the need for work-life balance which includes recruitment and retention of valuable work force, reduced employee stress, job satisfaction, reduced absenteeism, health benefits, and better life balance, by applying some interventions in the area of working hours which have been successful in improving work-life balance, such as, flexible working hours.

INTRODUCTION

Research over the past decades established that, work life balance has increased considerable concern and attention among trade unions, employers and scholars.

In the past, women were controlled to domestic tasks such as cooking, washing, cleaning, and caring children. They were labeled as home mothers and were denied the right or opportunity to leave the home. But things have changed recently. They have a significant function to engage in even outside the home, in addition to being a homemaker. Due to the increase in the number of nuclear families and rising living costs on the one hand and better education and employment prospects on the other, both husband and wife began to work, and many families became dual earners. Highereducation has enhanced women's work chances, allowing them to transition from home mothers to successful working professionals. Women have achieved significant progress in every profession and have left a permanent mark in their respective fields over time. However, there is no major difference in the way she performs her duties as a homemaker. In the vast majority of households, women continue to handle housework, cooking, care for family members and administer the household. Balancing both office work and family is a challenging task facing by women in the present scenario. The work-life balance of women employees is jeopardized when pressures at work and athome increase. The organization's expectations of its personnel are rising in this aggressive competitive environment. To meet the demands of the business, employees must extend themselves and focus more on their work, resulting in unbalanced work-life. In reality, establishing a balance between work and personal life is one of the most difficult situation that women employees facing in the twenty-first century. Many

female professionals in numerous industries are believed to have a disturbed work-life balance, which is contributing to an increase in divorces, worried family relationships and organizational conflicts. In today's world, the problem of work-life balance has become a burning topic. Changes in technology, values, and demographic trends all led to the growing importance of work-life balance in an industrialized cultures. Other reasons, such as the rising complexity of job, the changing role of family and the increased number of women entering the workforce also contribute to this. The difference between the demands of the workplace and the demands of personal life is referred to as worklife balance. Individuals and businesses suffer greatly as a result of a lack of synchronization between their personal and professional lives. Organizations are under pressure to attain high productivity in the competitive period and individuals with a healthy work-life balance are required, since an employee with a good work-life balance will be able to contribute more to the organization's growth and success. As a result, it is the moment for businesses to devise measures to assist female employees in liking their work and living life to the fullest. Any improvements in the workplace for female employees will benefit both the organization and also the employee.

Work-life balance is broadly defined as "an equally satisfied level of involvement or ‘fit’ among the multiple roles in a person’s life". In simple words, work life balance is all about people having a control over the work when, where and how they do. An effective work life balance assists a person in achieving both personal and professional goals.

This paper explores the literature related to work-life balance of women employees. Work-life balance confirms to be a necessity for personal satisfaction. Moreover, work-life balance has grabbed even more attention, as women increasingly enter to the business world. This is because for women, it is important but difficult to balance both their professional and the personal life.

STATEMENT OF THE PROBLEM

Once upon a time, the lines between work and family life were very clear. But today, work is about to occupy personal life and maintaining a balance between work and personal life is no longer an easy task. The reason for choosing this topic is to know the work environment and the personal environment of female employees and how they are able to manage both to perform their duties effectively at work place. Also to know the challenges they face at workplace.

OBJECTIVES OF THE STUDY

- To understand the work environment of female employees.
- To understand the personal environment (home environment) of female employees.
- To analyse the work life balance of female employees.

LITERATURE REVIEW

Based on earlier research and findings (for example, Schieman, and Glavin, 2008; Kamau, et al.,2013; Ojo et al., 2014; Oludayo, et al., 2015), there seems to be a relationship between work-lifebalance and different variables. Researchers around the world have carried out the studies on jobsatisfaction, role conflict, involvement, stress, commitment, workload, absenteeism, burnout,motivation, turnover, intention to leave, and so on, and directly or indirectly linked with professionaland personal life balance (Schieman, and Glavin, 2008; Kamau, et al., 2013; Oludayo, et al., 2015).

Work-life balance is responsible for shaping the attitude of employees and their personal lives(Oludayo, et al., 2015). Out of various factors which affect the efficiency of workers at theworkplace, work-life balance is one of them (Kamau, et al., 2013). Those having balanced careerand life most probably seem to be more effective in the work and vice versa. One of the challengesis to achieve a balance between family and personal life as it has greater influence on employees'work and life (Oludayo, et al., 2015).

Role conflict proposes that family and work domains are incompatible due to their different norms and responsibilities (Greenhaus and Powell, 2006; Omar et al., 2015). Thus, one could say thatexposure to stressors in a given domain, for example, work, might lead to fatigue, irritability, orpreoccupation with those problems, thereby limiting one's ability to meet the demands of otherdomains of life, for example, family, therefore, leading to work-family conflict (Ojo, et al., 2014).

In most societies, work-life conflict seems to be quite high especially in case of working women.This is because in majority of societies worldwide, women have traditionally shouldered the bulkof family responsibilities and remain primarily responsible for their children and the care of theelderly (World Bank, 2016). Thus, work life balance is seen more as women issue due to thetraditional mindset, where the woman is considered primarily responsible for the smooth running ofthe day to day affairs of the family irrespective of her job profile and official responsibilities. Thisexplains why managing work and family responsibilities can be very difficult for working women.(Omar et al., 2015; World Bank, 2016).

Schieman and Glavin (2008) found that, despite the fact that men also face this challenge ofbalancing work and other priorities, it affects women more since they do most of the work associatedwith the household activities, apart from taking care of older family members, children, and otherdependents. Although multiple roles in family and work can be the source of multiple satisfactionsfor employed women, a combination of family and career roles is often associated with conflict andstress. In addition, Rendon (2016) discussed that women usually suffer from the guilt-complex ofnot spending enough time during the tender age of their children and being forced to leave them forwork. Thus, women employees face a dual burden of work and family which creates role conflictand stress (Rendon, 2016). Similar findings were

reported in a study done by Hantrai (1990) thatshows the importance to working women being available for their children as much as possible. Theprice paid was the lack of personal time and the feelings of guilt, if any, free time was not used tobe with their children. Most women studied stated that they would sacrifice their own free time andreduce the amount of sleep they had so that their children did not feel the adverse effects of havinga working mother (Hantrai, 1990; Schieman and Glavin, 2008) be with their children. Most women studied stated that they would sacrifice their own free time andreduce the amount of sleep they had so that their children did not feel the adverse effects of havinga working mother (Hantrai, 1990; Schieman and Glavin, 2008).

Moreover, work-family conflict causes problems at home for women employees. These problemcan lead to increased frustration and stress for the person, which in turn can result in a decreasedsatisfaction with life. Likewise, when family issues follow the employee to the workplace, theworker can become preoccupied with these problems, causing new difficulties. (Hantrais andWalters, 1990). Consequently, conflicts in work-life balance of working women affects their healthas they tend to report more stress, muscle tension, headaches, weight gain and depression than theirmale counterparts (Oludayo, et al., 2015). Juggling between the obligations towards the familiesand expectations of the organization and constant struggle to maintain a balance between family andwork can have serious implications on the life of an individual by affecting their well-being as wellas overall quality of life There is a widespread demand from workers on the rightto balance home life and work in today's busy world where finding time for oneself seemsimpossible (Dreher, 2003).

Wellness and health programs can, for sure assist working women in balancing their personal andprofessional life (Roberts, 2005). However, these alone cannot be the answer to addressing the problems of imbalance (Dreher, 2003). The difficulties and problems of women aremultidimensional as evident from the literature reviewed; therefore, they require more probing toassist working women in balancing their family and work life (Roberts, 2005). There are manyfamily-friendly organizations that feel the need for work-life balance which includes recruitmentand retention of valuable work force, reduced employee stress, job satisfaction, reducedabsenteeism, health benefits, and better life balance (Baral and Bhargava, 2010). By applyinginterventions in the area of working hours which have been successful in improving work-lifebalance, such as flexible working hours (Roberts, 2005). Flexible working hours or self-rosteringcovers flexible start and finish times and a possibility for employees to request specific workinghours on a regular basis. Consequently, increased choice and control by the employee is enabled. increased influence has in several cases shown to increase work-life balance

An effectiveness of work-life balance practices and policies must incorporate theeffects of workplace culture and supervisor support of employee's efforts to balance family and workresponsibilities (Baral and Bhargava, 2010).

CONCLUSION

Work life balance is concerned as a vital issue nowadays for individual as well as organizations.Several factors are involved in determining the work life balance and imbalance of any individualwhich plays a critical role in women's personal and professional life. It is clear from the literatureabove that many antecedents of work life balance are found in many studies carried out in this area.Moreover, it has been explained that better work life balance creates several positive consequenceswhereas imbalance between work and family of an individual holds a negative effect which isresponsible for some serious issue for individual as well as for the organizations.

REFERENCES

Baral, R. and Bhargava, S. (2010) "Work–family enrichment as a mediator between organizationalinterventions for work–life balance and job outcomes", Journal of Managerial Psychology,25(3): 274–300.

CIPD. (2017) "CIPD people management awards". Available at: www.cipdpmas.co.uk/ [Accessed6 Jan 2020].

Clarke, M., Koch, L., and Hill E. (2004), "The work–family interface: Differentiating balance andfit". Family and Consumer Sciences Research Journal, 33(2).

Dreher, G., (2003), "The effect of work-life programs on female leadership at the top", HumanRelations, 40, 541-560.

Greenhaus, J., and Powell, G. (2006). "When work and family are allies: A theory of work-familyenrichment". Academy of Management Review, 31(1), 72-92.

Hantrais, L., and Walters, P. (1990). Gender Relations and Employment. The British Journal ofSociology, 41(3), 329-349.

Kamau, J., Muleke V, Makaya S., and Wagoki, J. (2013) "Work life balance practices on employeeperformance of Ecobank Kenya". European journal business and management,5(25), 179-185.

Konard, A., and Mnagel, R., (2000), "The impact of work-life programs on firm productivity",Strategic Management Journal, 21 (12), 1225-1235.

Rendon, R. (2016). "Work-Life Balance Among Working Married Women: What Social WorkersNeed to Know". Electronic Theses, Projects, and Dissertations.

Roberts, S. (2005). "Work/Life no longer a "woman's issue"". Business Insurance, 39 (32), 3-4.

Schieman, S., and Glavin, P. (2008). "Trouble at the border? Gender, flexibility at work, and thework home interface". Social Problems, 55(4), 590-611.

Ojo, I., Falola, H., and Mordi, C. (2014) "Work life balance policies and practices: A case study ofNigerian female university students". European Journal of Business and Management, 6(12), 184-193

3D PASSWORD TECHNOLOGY: ENHANCING AUTHENTICATION AND SECURITY IN THE DIGITAL ERA

[1]Ashish Mishra, Assistant Professor (MCA Dept.), Jagran Institute of Management,Kanpur, E-mail_id:kanpur.ashish@gmail.com
[2]Adarsh Srivastava, Assistant Professor (MCA Dept.), Jagran Institute of Management,Kanpur, E-mail_id:adarsh.srivastava1984@gmail.com

ABSTRACT

As the digital landscape expands and becomes increasingly interconnected, ensuring robust security measures for user authentication has become a critical concern. Traditional password-based authentication systems suffer from various vulnerabilities, such as password cracking, shoulder surfing, and phishing attacks. In response to these challenges, 3D password technology has emerged as a promising approach to strengthen user authentication and enhance security. This research paper provides an overview of 3D password technology, its underlying principles, and its potential applications. It explores the advantages and limitations of this technology, highlights recent advancements, and discusses future research directions. The paper concludes by emphasizing the importance of adopting innovative authentication mechanisms like 3D passwords to address the evolving security threats in the digital era.

1. INTRODUCTION

3D password technology is an innovative approach to enhance the security of user authentication systems. Unlike traditional password-based methods, the 3D password employs a multi-factor authentication system that incorporates three-dimensional virtual environments. Users are required to interact with these virtual environments by selecting and manipulating various objects, such as shapes, colors, and movements, to create a unique and personalized authentication sequence. This technology aims to overcome the limitations of traditional passwords by adding an additional layer of complexity and making the authentication process more intuitive and secure. By leveraging the spatial awareness and cognitive abilities of users, the 3D password technology offers a promising solution to strengthen the security of digital systems.

1.1 TRADITIONAL PASSWORD-BASED AUTHENTICATION SYSTEMS

Traditional password-based authentication systems are one of the most common methods used to verify the identity of users and grant access to various systems and services. In such systems, users are required to provide a unique combination of characters (i.e., a password)

that matches the stored password associated with their account. Here are the key elements and characteristics of traditional password-based authentication systems:

- **Username:** A unique identifier used to associate the password with a specific user account.
- **Password:** A secret combination of characters chosen by the user to authenticate their identity. The password is typically required to be confidential and known only to the user.
- **User database:** A repository where user credentials, including usernames and corresponding passwords, are stored. The user database may be implemented using various technologies such as file-based storage, relational databases, or directory services.
- **Authentication process:** When a user attempts to log in, the authentication process compares the provided username and password with the corresponding entry in the user database. If the entered password matches the stored password, the user is granted access.
- **Password hashing:** To enhance security, passwords are often not stored directly but instead are transformed into a cryptographic hash using algorithms like MD5, SHA-1, or bcrypt. The hashed passwords are then stored in the user database. During authentication, the entered password is hashed and compared against the stored hash.
- **Password policies:** Password-based authentication systems often enforce certain policies to enhance security. These policies may include requirements such as minimum length, the use of a combination of letters, numbers, and special characters, regular password changes, and restrictions on reusing old passwords.
- **Password strength:** The strength of a password refers to its resistance against various attacks. Strong passwords are typically long, complex, and unique, making them harder to guess or crack through brute-force or dictionary attacks.
- **Single-factor authentication:** Traditional password-based systems typically rely on single-factor authentication, meaning that only the password is required to prove the user's identity. This can be a limitation since passwords can be forgotten, stolen, or easily guessed, potentially leading to unauthorized access.
- **Security challenges:** Traditional password-based systems face several security challenges, such as the reuse of passwords across multiple accounts, weak password choices, social engineering attacks (e.g., phishing), and the risk of password database breaches.
- While password-based authentication remains widely used, there is a growing recognition of its limitations and the need for additional security measures. As a result, many systems are adopting or supplementing traditional passwords with

additional authentication factors, such as two-factor authentication (2FA), biometrics, hardware tokens, or password less alternatives, to enhance security and user experience.

1.2 VULNERABILITIES AND LIMITATIONS

Here are some of the common weaknesses associated with such systems:

- **Weak Passwords:** Users often choose weak passwords that are easy to guess or crack. These include common words, personal information, or simple patterns, making them vulnerable to brute-force attacks or dictionary attacks.
- **Password Reuse:** Many users reuse passwords across multiple accounts, which increases the risk of compromise. If one account is breached, attackers can gain access to other accounts using the same password.
- **Social Engineering:** Password-based systems are susceptible to social engineering attacks, where an attacker manipulates or tricks a user into revealing their password. Techniques like phishing emails, phone calls, or fake websites are used to deceive users into disclosing their login credentials.
- **Shoulder Surfing:** Passwords can be stolen through observation. An attacker may simply watch the user enter their password, either directly or through video surveillance, compromising the account's security.
- **Password Storage:** Traditional systems store passwords in databases, often in hashed or encrypted forms. However, if an attacker gains unauthorized access to the database, they can potentially retrieve the passwords or crack the encryption, compromising the entire user base.
- **Lack of Two-Factor Authentication (2FA):** Passwords alone provide a single layer of security. Without additional factors, such as a verification code sent to a mobile device, the system is more vulnerable to unauthorized access.
- **Password Resets:** Password reset mechanisms that rely on security questions or email verification can be compromised. If an attacker gains access to the user's email account or knows the answers to security questions, they can reset the password and gain unauthorized access.
- **Insecure Communication:** Passwords can be intercepted during transmission if the communication between the user and the authentication server is not adequately secured. This vulnerability can be exploited through techniques like packet sniffing or man-in-the-middle attacks.
- **Lack of User Awareness:** Users may not be aware of the importance of strong passwords, password hygiene, or the risks associated with sharing or disclosing passwords, making them more susceptible to compromise.

- **Account Lockouts:** Traditional systems often implement account lockouts after a certain number of failed login attempts. While this is intended to enhance security, it can also be exploited by attackers to lock out legitimate users or conduct denial-of-service attacks.

2. INTRODUCTION TO 3D PASSWORD TECHNOLOGY

3D Password technology is an authentication method that enhances security by incorporating the spatial dimension. Users interact with a 3D virtual environment to set and enter their passwords, utilizing the combination of traditional alphanumeric passwords, graphical passwords, and gestures for more robust authentication.

2.1 DEFINITION AND CONCEPT

This can be done by designing a 3D virtual environment inside a 2D screen that contains objects such as text, graphical icons, virtual gestures, sound, touch, voice commands that request information to be remembered and recognized, as well as authenticate tokens and biometric data. In the virtual 3D environment following virtual objects can be considered as a part of the 3D password - A fingerprint reader, a computer with which the user can type; a light that can be switched on/off, any graphical password scheme, any real life object etc.

The user is presented with virtual environment where the user navigates and interacts with various virtual objects and the systems observe the series of actions and interactions with the objects inside the 3d environment and these activities by user helps to constructs the user's 3d password. These passwords are Highly Secure, Easy to remember, Easy to customize, Eliminates Brute Force Attack, Difficult to guess and share and has No specific size limit.

2.2 COMPONENTS OF 3D PASSWORDS

A 3D password is a type of authentication scheme that incorporates three-dimensional objects or virtual environments as a means of authentication. It aims to provide an additional layer of security beyond traditional password-based authentication methods. The components of a 3D password typically include the following:

1. **Text-based Password:** This component is similar to a traditional alphanumeric password. Users are required to enter a combination of letters, numbers, and symbols to authenticate their identity. It serves as the initial layer of security.
2. **Graphical Password:** This component involves using graphical objects or images as a password. Users may be asked to select a particular pattern, sequence, or location on a pre-defined image or set of images to establish their identity.
3. **Biometric-based Authentication:** This component utilizes biometric characteristics of individuals to authenticate their identity. Biometric features like fingerprints, iris scans, voice recognition, or facial recognition can be incorporated into the 3D password system to enhance security.

4. **Virtual Reality (VR) Environment:** This component involves using a virtual reality environment for authentication purposes. Users navigate and interact with a 3D virtual environment to establish their identity. The VR environment may contain objects, puzzles, or challenges that the user needs to navigate through successfully.
5. **Personalized Objects:** This component allows users to select or create their personalized 3D objects or models. These objects can be associated with specific actions or behaviors to authenticate the user. For example, a user may be required to rotate, manipulate, or interact with their personalized object in a particular way to gain access.
6. **Contextual Information:** Contextual information refers to additional data or environmental factors that can be used for authentication. This can include location-based information, time of access, device characteristics, or other contextual cues that help verify the user's identity.

The combination and implementation of these components can vary depending on the specific 3D password system or application. The aim is to create a multi-factor authentication mechanism that combines the strengths of different authentication methods to enhance security and protect against unauthorized access.

3. HOW 3D PASSWORDS WORKS

3D passwords work by combining multiple factors and authentication mechanisms to enhance security and provide a more robust authentication process. Here's a general overview of how 3D passwords typically work:

1. **User Registration:** The user goes through a registration process to establish their identity in the 3D password system. This may involve creating a text-based password, selecting graphical objects, providing biometric information, or personalizing 3D objects.
2. **Authentication Setup:** During the setup phase, the user defines their authentication factors and preferences. This includes selecting the types of authentication components they want to use, such as text-based passwords, graphical passwords, biometrics, or virtual reality environments.
3. **Login Process:** When the user attempts to log in, they provide their username or identifier to initiate the authentication process.
4. **Authentication Factors**: The user is prompted to provide the various authentication factors they have chosen during the setup phase. This typically includes a combination of text-based passwords, graphical password inputs, biometric scans, and interactions with 3D objects or virtual environments.
5. **Authentication Validation:** The system validates the provided authentication factors against the user's registered data. This involves checking the correctness of the text-based password, verifying the accuracy of the graphical password input,

comparing biometric information with the registered data, and assessing the user's interactions with 3D objects or virtual reality environments.

6. **Access Granted or Denied:** Based on the successful validation of the authentication factors, the system determines whether to grant or deny access to the user. If all the factors are authenticated successfully, the user is granted access to the protected system or resource.

The strength of the 3D password lies in the combination of multiple authentication factors, making it more challenging for an attacker to compromise the system. Even if one factor is compromised, the other factors act as additional layers of security.

It's important to note that the implementation details of 3D passwords can vary depending on the specific system or application. The components used, the sequence of authentication factors, and the level of integration with existing authentication infrastructure may differ. Additionally, 3D passwords may also incorporate additional security measures like encryption, session management, or anti-fraud techniques to further enhance the overall security of the system.

4. ADVANTAGES AND LIMITATIONS OF 3D PASSWORDS

4.1 ADVANTAGES

Enhanced Security: 3D passwords offer a higher level of security compared to traditional text-based passwords alone. By incorporating multiple authentication factors such as text-based passwords, graphical passwords, biometrics, and virtual reality environments, the system becomes more resistant to unauthorized access and password guessing attacks.

Increased User Engagement: The interactive nature of 3D passwords, such as navigating through virtual environments and interacting with personalized objects, can enhance user engagement. This can lead to a better user experience and potentially higher user satisfaction compared to traditional password-based systems.

Multi-Factor Authentication: 3D passwords provide multi-factor authentication, combining various authentication factors into a single system. This makes it more difficult for attackers to bypass the authentication process, as they would need to compromise multiple factors simultaneously.

Resistance to Shoulder-Surfing Attacks: Traditional password systems are vulnerable to shoulder-surfing attacks, where an attacker observes the user's password input. In 3D passwords, graphical elements and interactions with personalized objects add an additional layer of complexity, making it harder for an attacker to observe and replicate the authentication process.

4.2 LIMITATIONS:

User Familiarity and Training: Implementing 3D passwords requires users to adapt to new authentication methods and interfaces, such as navigating virtual environments or interacting

with 3D objects. This may require additional training and familiarization, which can be a barrier to user acceptance and adoption.

Implementation Complexity: Developing and deploying a 3D password system can be complex, especially when integrating multiple authentication components and ensuring compatibility with existing infrastructure. It may require significant resources, expertise, and technical support.

Usability and Accessibility: Some users may find 3D passwords less intuitive or more challenging to use compared to traditional text-based passwords. It may also pose accessibility challenges for users with disabilities, such as those with visual impairments who rely on screen readers or individuals with limited dexterity for interacting with 3D objects.

Potential Security Risks: While 3D passwords offer enhanced security, they are not immune to potential vulnerabilities. Like any authentication system, 3D passwords can be subject to attacks such as social engineering, biometric spoofing, or vulnerabilities in the implementation itself. Regular security assessments and updates are necessary to mitigate these risks.

Overall, 3D passwords provide a promising approach to strengthen authentication systems. However, their successful implementation and adoption require addressing usability concerns, ensuring proper training and support for users, and continuously addressing security challenges.

CONCLUSION

3D password technology offers a promising approach to enhance security in digital systems by incorporating a multi-factor authentication system. It employs a combination of traditional authentication factors, such as passwords and PINs, with spatial and temporal dimensions. By utilizing 3D virtual environments, users can create personalized and unique authentication scenarios based on their spatial and temporal behaviors, making it difficult for attackers to replicate or guess. However, while 3D password technology shows potential in improving security, it still faces challenges in terms of user acceptance, implementation complexity, and potential vulnerabilities. Further research and development are needed to address these issues and realize its full potential as a secure authentication mechanism.

REFERENCES:

1. Moniri, M. M., & Abdullah, M. R. (2013). 3D password: A survey of authentication schemes and protocols. Journal of Network and Computer Applications, 36(1), 1-11.
2. Jain, A., Jain, R., & Jain, R. (2013). A survey on 3D password schemes for authentication. International Journal of Computer Applications, 62(9), 13-17.
3. Kaur, H., & Bala, M. (2015). Comparative analysis of 3D password authentication techniques. Procedia Computer Science, 57, 1019-1026.

4. Chakraborty, S., & Dasgupta, S. (2017). An overview of 3D password: A graphical password authentication system. International Journal of Computer Science and Information Security, 15(9), 75-79.
5. Jain, R., Verma, R., & Vyas, O. P. (2014). A survey of 3D password authentication schemes. Procedia Computer Science, 48, 768-773.
6. Mansouri, A., Taleb, N., & Alasiry, A. (2019). An efficient three-factor authentication scheme based on 3D password. Computers & Electrical Engineering, 75, 45-56.
7. Mondal, M., & Gope, M. (2016). 3D password authentication: A comprehensive study. In 2016 International Conference on Information Technology (ICIT) (pp. 10-14). IEEE.
8. Velusamy, R., & Gopalan, N. (2016). A survey on graphical password authentication schemes using 3D password. International Journal of Engineering and Technology, 8(2), 722-727.

Cognitive Computing: Transforming Cyber security Through Advanced Threat Detection and Response

[1]Mr. Anand Kumar Dixit, Assistant Professor, Jagran Institute of Management, acheiveranand@gmail.com
[2] Dr. Anil Kumar Singh,Professor & Dean Jagran Institute of Management, Kanpur, anil.sysadmin@gmail.com

ABSTRACT:
With the advancement technology, the threats posed by it have also evolved over time. Cyber-crimes have become very common today and have also evolved over the years. Thus, the need for cybersecurity is now more than ever. Cybersecurity, in simple terms, refer to the practice of protecting our system from the cyber-attacks. There are several ways that have been in use for preventing or avoiding these attacks to be made on an individual or an organisation. This paper discusses the use of machine learning in promising cybersecurity to the organisation and the individuals. Machine learning can be defined as the ability of computers to learn from the data or information available and accordingly perform an action. This concept of machine learning can prove to be beneficial in keeping the users secure from the cyber-attacks by analysing the repeated behaviour or pattern of these cyber-attacks. The paper also talks about how machine learning has been useful for maintaining the cybersecurity of the systems. It elaborates the various ways in which it can be used in the organisations to help prevent them the cyber-attacks.
KEYWORDS: Cognitive Computing , Machine Learning, Cyber security, Cyber-crime, Cyber-attack

1. Introduction :

Cognitive computing refers to the field of computer science that aims to create systems capable of simulating human thought processes and intelligent behaviour. It involves the development and deployment of computer systems that can understand reason, learn, and interact with humans in a natural and human-like manner.

Cognitive computing systems utilize various techniques such as natural language processing, machine learning, knowledge representation, and data mining to analyze vast amounts of data, extract meaningful insights, and make informed decisions. These systems are designed to mimic human cognitive abilities, including perception, language understanding, problem-solving, and decision-making.

The goal of cognitive computing is to enable machines to augment human intelligence, assisting in complex tasks, providing personalized recommendations, and aiding in decision-making processes across various industries and domains, including healthcare, finance, customer service, and scientific research. By leveraging advanced algorithms and cognitive models,

cognitive computing strives to bridge the gap between human and machine intelligence, unlocking new possibilities for data analysis, automation, and problem-solving.

2. Cyber security :

While Cyber security is the practise of defending systems, networks, and programmes from cyberattacks. These cyber-attacks include disrupting normal business operations, extorting payment from users, or accessing, altering, or deleting important data. In words of Fredrick Chang, cyber security is defined as – *"*A science of cybersecurity offers many opportunities for advances based on a multidisciplinary approach, because, after all, cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines. So, in addition to the critical traditional fields of computer science, electrical engineering, and mathematics, perspectives from other fields are needed." (Craigen, 2014). Cybercrimes date back to even the prior days of internet. However, the level of crimes observed have evolved since then with the evolution of computers and internet. And today, the need of cybersecurity has increased now more than ever. It is challenging to put effective cybersecurity safeguards in place in the modern world since there are more devices than people and hackers are becoming more inventive. Machine learning plays vital role in cyber security.

3. Machine learning :

Machine learning can be defined as a branch of computer science which enables computers to learn instead of being programmed. "Its origin can be traced back to artificial intelligence movement that took place in 1950s"(Bi et al., 2019). in simple words in machine learning computer learns while performing the tasks through "experience" which usually means fitting to data. A simple idea that developed in 1950s has now been fuelled with advances in computer science and statistics as well as better datasets. In recent times machine learning has unknowingly become part of our lives. we can simply trace its presence in automated translation, image recognition, voice search technology, self-driving cars and beyond.It is even entering the field of cybersecurity and will soon become an integral part of it. Machine learning over the years has proved to be helpful for tackling cybercrimes and there would be many possible ways in future for the same.

4. Use of cognitive approach :

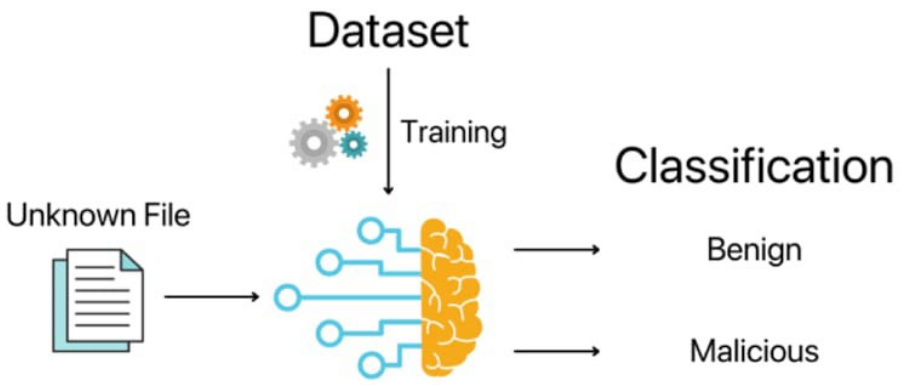
It can be used by cybersecurity systems to look for patterns and learn from them in order to stop similar attacks and respond to changing behaviour. It can help cybersecurity teams stop threats earlier and respond to ongoing attacks more rapidly. It can reduce the amount of time spent on repeated tasks and enable businesses to use their resources more effectively. In summary, machine learning may greatly improve cybersecurity by making it less complicated, more proactive, and less expensive. But it can only carry out such tasks if the machine learning is

supported by data that fully captures the environment. Garbage in, garbage out, as the saying goes.

Enterprises can only face the challenge of cybersecurity now and in the future with the help of machine learning, which can identify complex events and scenarios at scale. This is due to the fact that there aren't sufficient human security resources whereas there are more devices and threats online every day. The scope of machine learning in cybersecurity is quite obvious for those who know the wonders of machine learning.

Effective cyber security application is made possible by machine learning. For an IT organization it is impossible to be aware of every device that is being connected to a given network which might pose a great hindrance to functioning of the organization.In this difficult situation, machine learning can be of great help. Machine learning can be used to profile these devices, thereafter judging features and behaviour of given device.

Development of security policies for an organisation is usually hectic task. Manually, it would take a lot of time and work to build those policies, which can be made easy with machine learning. Since, it already knows the profile and behaviour of the devices connecting to the organisation, therefore, it would be easy for the machine learning to develop the security policies accordingly and even provide accurate solutions for the same" (Dr. May Wang, CTO of IoT Security at Palo Alto Networks and the Co-founder, Chief Technology Officer (CTO), and board member of Zingbox, 2022).



Machine learning is a hottest trend in today's market, and it is predicted that by 2025 nearly 50% of the products are based on machine learning. ML is a subclass of AI and it is a technique where machines learn automatically from past experiences and not being programmed for it explicitly. It uses statistical methods to enable machine to improve experience. It is a core of many technologies advancement like self driving car by Tesla, face reorganization in apple iphone etc.

ML algorithms tend to make a mathematical model which is based on sample data technically known as “training data”. The model is used further to make decisions and predictions based on that training data and are not being programmed explicitly to do such tasks. Sun et al. [3] surveys various techniques of machine learning and its application in wireless networks.

5. Classification of Machine Learning:

5.1. Supervised Machine Learning:

In supervised machine learning, the machine is trained using labeled training data. Here trainer is having input data and as well as output data that is called astraining data .The machine is trained with training data under supervision of trainer. Learning will stop when machine will achieve an acceptable level of performance. Finally, machine is ready to predict the output for any new set of input data.

For example: Suppose that in an organization biometric machine is trained by giving the thumb Impressions of an employee in a different angle. Once machine is trained it will labeled that impression with employee name or employee ID and in future employee will be easily identify with his thumb impression.

5.2. Unsupervised Machine Learning:

In this type of machine learning machine is trained by unlabeled data. In unsupervised learning we have only input data no output data is available. Training data is grouped in a different cluster based on their characteristics and each cluster is labeled.

For example: Suppose that we have data of some cricketers like name, total run scored and number of wickets taken. Trainer will train the machine in such a way that if any cricketer scored more runs but took fewer wickets labeled as batsman and if scored less runs and took more wickets labeled as a bowler. So, in future machine will easily predict either cricketer is batsman or bowler.

6. Reinforcement Machine Learning: It is also called as semi-supervised machine learning. In this type of machine learning large amount of input data is available but only some of the data is labeled. This method is lying between supervised and unsupervised learning. It is based on reward based learning or work on the principle of feedback.

For example: Suppose that trainer will give dog image as input to machine and check whether machine identifies it or not. If machine will identify it as cat image trainer will give negative feedback to machine by saying it is a dog image. So, next time when there is input of dog image machine will identify easily.[4][5]

Machine learning is not a new concept for hackers either, many hackers are using it for finding loopholes in security systems of organizations and hacking devices for stealing confidential information. It’s high time the organization act with the motive of eye for an eye. An organization has to handle a large number of connection requests on daily basis and at the same

time look for suspicious activities such as one involving receiving and sending of large amount of information. Presently this work is handled by personnel working in the organization who are vulnerable to inaccuracy. This is when machine learning comes into picture. A right combination of machine learning and artificial intelligence clubbed with cyber threat identification system can be a great help in monitoring all outgoing and incoming calls along with all requests to system in order to detect any suspicious activity.

Another area where machine learning can be used is to prevent phishing attacks. Every day a large number e-mails are sent and received through e-mail accounts of employees. a common practice adopted by hackers is to send fraudulent mails to employees asking them about their sensitive information such as banking and credit card details. These phishing traps can be avoided by installing cyber security software along with machine learning. This software will act as a watch dog and closely monitor e-mail accounts of employees and immediately report any suspicious activities.

7. Cognitive Computing: It can play a crucial role in enhancing cyber security measures by providing advanced capabilities for threat detection, analysis, and response. Here are several ways in which cognitive computing can help in the field of cyber security:

7.1. Threat Detection: Cognitive computing systems can analyze vast amounts of data, including network traffic, system logs, and user behavior, to identify patterns and anomalies that may indicate potential security threats. By continuously monitoring and analyzing data in real-time, cognitive systems can detect and flag suspicious activities or deviations from normal behavior, helping to identify potential cyber threats at an early stage.

7.2. Intelligent Analytics: Cognitive computing can perform advanced analytics on cyber security data, including threat intelligence feeds, vulnerability databases, and historical attack data. By applying machine learning algorithms, these systems can identify patterns, correlations, and trends that may be indicative of emerging threats or vulnerabilities. This can aid in proactive threat mitigation and allow security teams to take preventive actions to safeguard systems and networks.

7.3. Automated Response: Cognitive computing systems can automate certain aspects of cyber security incident response. By leveraging predefined rules, machine learning models, and real-time analysis, these systems can automatically trigger responses to mitigate or contain threats. For example, they can block suspicious IP addresses, quarantine infected devices, or initiate incident response workflows. Automated response capabilities can significantly reduce response times, allowing security teams to address threats swiftly and efficiently.

7.4. Natural Language Processing: Cognitive computing systems equipped with natural language processing capabilities can analyze unstructured data sources such as security blogs, forums, and social media to gain insights into emerging threats, vulnerabilities, and attack

techniques. By extracting and analyzing information from various sources, these systems can provide security teams with real-time intelligence and situational awareness, enabling them to respond effectively to evolving cyber threats.

7.5. User behaviour Analysis: Cognitive computing can assist in detecting insider threats by monitoring and analyzing user behaviour across an organization's digital ecosystem. By establishing baselines of normal behaviour for individual users and systems, cognitive systems can identify anomalous or suspicious activities that may indicate unauthorized access or malicious intent. This helps in identifying potential insider threats and taking appropriate actions to mitigate risks.

8. Conclusion:

In the recent decades, we have witnessed the evolution of cybercrimes with the advancement of technology. The risks of technology have increased with this evolution and it is the need of the hour to use the advanced techniques to tackle these cyber-attacks. Machine learning, being one of the most powerful tools available to us, has proved to be useful in detecting cyber-crimes through the machine learning algorithms. The use of machine learning in cybersecurity is no secret from the world. It has proved to be pf great help to prevent these cyber-attacks. However, the use of machine learning algorithms in cybersecurity to prevent the attacks on the system is still quite new. Therefore, the precision with which these attacks need to be identified is yet not achieved but constant research in the field would help to minimise the false detections of machine learning and thus, the accuracy would be achieved.

In summary, cognitive computing brings advanced analytics, real-time monitoring, automation, and intelligent response capabilities to cyber security. By leveraging these capabilities, organizations can enhance their ability to detect, analyze, and respond to cyber threats effectively, ultimately strengthening their overall security posture.

References:

1. Dr. May Wang, CTO of IoT Security at Palo Alto Networks and the Co-founder, Chief Technology Officer (CTO), and board member of Zingbox. (2022, September 23). The Future of Machine Learning in Cybersecurity. CIO. https://www.cio.com/article/406441/the-future-of-machine-learning-in-cybersecurity.html
2. Bi, Q., Goodman, K. E., Kaminsky, J., &Lessler, J. (2019, December 12). What is Machine Learning? A Primer for the Epidemiologist. https://academic.oup.com/. https://academic.oup.com/aje/article/188/12/2222/5567515
3. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10).

4. Anand kumar Dixit, “Power of blending the Internet of Things (IoT) and Machine learning”, Jagran J. mgt. and tech., August,2020.
5. Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, andApplications," Journal of Electrical and Computer Engineering, Hindawi, 2017, https://doi.org/10.1155/2017/9324035
6. Shadi Al-Sarawi, Mohammed Anbar , Kamal Alieyan , Mahmood Alzubaidi, "Internet of Things (IoT) communication protocols: Review, " 8th International Conference on Information Technology (ICIT), IEEE, 2017, DOI: 10.1109/ICITECH.2017.8079928.
7. The Cognitive Perspective on Learning: Its Theoretical Underpinnings and Implications for Classroom Practices, August 2011,The Clearing House: A Journal of Educational Strategies, Issues and Ideas 84(5):204-212,
DOI: 10.1080/00098655.2011.568989
8. Cognitive approaches to emotions,January 2014,Trends in Cognitive Sciences 18(3)
DOI:10.1016/j.tics.2013.12.004

Indian Derivative Market

Dr. Meenakshi Jaiswal, Assistant Professor, Jagran Institute of Management, Email: meenu067@gmail.com

Introduction The world has witnessed growth in international trade and business due to liberalisation in the past couple of years. This resulted in increased demand for international currency, financial instruments and fluctuation in interest rates, exchange rates and market-linked securities. These developments have exposed the financial markets to high risk and volatility. To combat with the adverse effects of a volatile market and manage the risk, new products called derivatives were developed. Anyone who is active in the financial world must have heard about the term 'Derivatives'. In simple terms, derivative is a contract between two parties whose value is derived from the value of underlying asset based on which the contract is made. To understand the concept of derivative, let us take a simple example of AA Co. Ltd., a manufacturer of potato chips. The price of the potatoes is fluctuating in the open market and the manufacturer wants to lower the risk. Hence, instead of purchasing potatoes in a spot market, he enters into a forwards contract with the farmer that AA Co. Ltd., will purchase potatoes at a specific rate on some future-specific date from the farmer. In this case, AA Co. Ltd., and the farmer are the parties to the derivative contract. The value of the contract is dependent upon the value of the potatoes. Derivatives (as it is referred to instead of derivative) have originated to ensure stability in exchange rates. The collapse of fixed exchange rates of currencies globally, the foundation for foreign exchange derivatives were laid during the initial period of 1970s. Equity derivatives originated in the later period of 1980s. With the application of Black and Scholes model, the pricing of derivative gained significance globally.

Keywords:- Derivatives, exchange rates, price, contract, underlying asset

In India, derivatives are used increasingly by various market players like brokers, dealers, Central Government and State Governments, corporate treasures, individual investors, etc. This chapter includes all basic concepts related to derivatives, derivative contracts and its mechanism.

Daily turnover of NSE derivatives?

On a monthly basis, the NSE recorded an average daily turnover of **Rs 68,013 crore** during April 2022, the highest for FY23; the lowest was Rs 44,608 crore for June 2022. The highest average in FY22 was Rs 81,361 crore for October 2021, while the lowest was Rs 53,597 crore for December 2021.

Derivatives: "It is a financial instrument whose value is derived from the underlying asset".

So derivatives are financial products which have no independent values. The value of derivatives is derived from the value of another financial instrument to which they are linked. For example, in case of Nifty futures, Nifty index is the underlying asset.

As per the Indian Securities Contracts (Regulation) Act, 1956, derivatives include:

1. Security derived from a debt instrument, share, loan (whether secured or unsecured), risk instrument or contract for differences or any other security.
2. A contract which derives its value from the prices or index of prices from the underlying securities.

Derivatives can be either a financial derivative or a commodity derivative depending on the underlying asset. If the underlying asset is a commodity, then it is commodities derivatives; if the underlying asset is a financial instrument, then it is financial derivatives.

An underlying asset

The underlying asset is a financial instrument or a commodity on which the value of the derivative is dependent. In simple words, we can say that it is an asset on which the derivative contract is written.

Following are some of the examples of an underlying asset:

a. Stocks and share warrants
b. Currency
c. Index
d. Interest rates
e. Commodities
f. Money market products
g. Short-term securities
h. Bonds

Features of underlying assets:

Following are the important features of an underlying asset.

a. The value of an underlying asset changes continuously.
   For example, currency is an underlying asset whose value fluctuates in the financial market.
b. The value of the derivative is directly or inversely related to the price of the underlying asset.
   For example, Put Option; if put option is entered by the option holder for a particular share, the value of which plummets during the option period, the put option demand increases with the fall of the concerned share price.

Implication of an Underlying Asset:

Derivative contracts are entered mainly because of following two reasons:

• To hedge against fluctuation in price of the underlying asset

• To speculate

In both the cases, implication of underlying assets is the same. For example, on 1st October 2016, an investor purchases100 shares of IndusInd Bank Ltd. for 1200. It is expected that the value of the share will go down in future. Hence, the investor buys a put option (an option to sell shares at a particular price) to safeguard against loss due to price fluctuation at a strike price of 1,275 per share after two months. On 1st December, 2016 the share price drops in the market and hovers around 1,000 per share. The investor exercises the option and sells the shares at 1,275 on that date. Thus, he hedges himself from the loss due to decline in value of the underlying asset.

Similarly, a speculator apprehending a drop in price of IndusInd bank takes a long position with put options in the market on 1st October, 2016 for 1000 shares. At the end of two months when there is decline in the share price below the strike price (the price at which the option will be exercised), he closes the position and realises the gain (difference between strike price and market price).

Thus, hedgers use the derivative market to avoid exposure to adverse movements in the price of the underlying asset, whereas, speculators take position in the market based on such movements in the price of that asset. It is clear from the above example that the profit and loss positions of the derivative contract are wholly dependent upon the value of the underlying asset.

Advantages of Derivatives

• **Leverage Returns:** The most important and attractive feature of the derivatives is their leveraging of returns effect. An investor can earn high returns that may not be possible if he would have invested in any of the underlying asset. To understand it better, we can take the example of a stock. The current stock price of XYZ Ltd. is `40 which is expected to move up in the next three months. An investor has `10,000 to invest. The value of three-month call with a strike price of ` 50 is ` 2.50. If he purchases shares, he can purchase only 250 shares (10,000/40). If he invests in call option, he can control 4,000 shares (10,000/2.50). After 3 months, the share price moves to `45. In case of 1st option, gain to the investor is (45-40)*250, i.e., `1,250. In case of 2nd option, the gain to the investor is (45-40-2.5)*4,000, i.e., `10,000. Thus, it is observed that derivative market can increase the return of an investor many folds with the same investment. Thus, the effect of increase of price of a stock by one unit may cause increase in value of derivatives more than the stock.

• **Non-binding Contract:** PuPurchasing a derivative contract like options means purchasing the right to exercise it. It is up to the purchaser whether to exercise the right or not. It is not an obligation. Hence, it gives too much flexibility to the investor.

• **Hedging against Price Fluctuations**: The price of a financial instrument fluctuates due to various reasons. The factors for price variation may be demand and supply ratio of an asset, political and economic situations, interest rate fluctuation, exchange rate fluctuation, etc. It is difficult to estimate the future price correctly. Here, derivatives can be used to hedge against the future price fluctuations.

• **Return without Physical Settlement:** Derivative contracts are not always physically settled. For example, a stock price is currently trading at `100. Call option with six months to expiration and an exercise price of `100 are trading at `10.90. A trader is of the opinion that the market will rise over the next six months and decides to speculate by taking a long position in three contracts. Assume that the stock price rises to `110 after a few weeks and the corresponding value of the option is `16.65. In this case, the trader can exit with a profit by offsetting his position: 3*100*(16.65-10.90) = `1,725.

• **Transfer of Risk:** Derivative allows investors re-distribution of risks by shifting and managing efficiently different types of risks through hedging, arbitraging and spreading. They can be used to protect against specific exposure like interest rates fluctuations, price fluctuations, volatile exchange rates and monetary turmoil.

• **Arbitrage Trading**: Through arbitrage trading, market makers buy and sell futures contracts hoping of profit from price differentiation between two markets. For example, at an expiration of gold in a three-month futures contract, the future price is `30,000 per 10 grams, and the spot price is `28,680 per 10 grams. An arbitrageur can make spot purchase and go short for three months futures contract. He makes a profit of `1,320 per 10 grams in absence of transaction costs.

Conclusion of Derivative

- **Derivatives** is a 'financial product' whose value is derived from the underlying asset.
- The underlying asset is a financial instrument or a commodity on which the value of the derivative is dependent.
- Literally, there are thousands of derivatives available in the market, but the essence of all of them is a forward, futures, an option or a SWAP contract.
- Derivative trading is primarily made up for financial experts, professional money managers and highly experienced investors.

- A forward contract is entered between two parties to buy or sell a specified quantity of an asset at a certain future date at a specified price agreed now.
- Futures contract is a standardised forward contract which is traded on an exchange in which it is registered.
- Option is a derivative contract which gives the option holder a right but not obligation to exercise his option.
- Derivative has evolved from 1600s in the Dutch Market to SWAPS, OTC, Futures in late 80s to a wide variety we come across today.

Bibliography /reference:-

e-References

1. Derivatives Basics | Types of Derivatives | FAQs | BSE. (2017). Bseindia.com. Retrieved 2 January 2017, from http://www.bseindia.com/markets/Derivatives/DeriReports/FAQsBasicsofDerivat ives.aspx
2. History of Derivatives (2017). Sebi.gov.in. Retrieved 2 January 2017, from http://www.sebi.gov.in/commreport/LC04.html
3. Questions on Derivatives (2017). Sebi.gov.in. Retrieved 2 January 2017, from http://www.sebi.gov.in/faq/derivativesfaq.html
4. Facts about NSE (2017). Retrieved 2 January 2017, from https://www.nseindia.com/research/dynaContent/nsefactbook2016.pdf

External Resources

1. John C Hull and Sankarshan Basu. (2014), Options, Futures, and Other Derivatives. 9th Edition. Pearson
2. Sunil Parameswaran. (2010) Futures and Options-Concepts and Applications. (1stEdition), McGraw-Hill Education
3. Neil C. Schofield. (2007). Commodity Derivatives: Markets and Applications, Wiley Finance
4. Introduction to Financial Derivatives(Link https://www.youtube.com/watch?v=yTxxSTXg404)
5. Types of Derivatives (https://www.youtube.com/watch?v=r1s115EBydM)
6. Financial Derivatives: (Explained https://www.youtube.com/watch?v=nf9ByTdX0a)

The Study of Artificial Intelligence And Its Practice In Management

[1]Ms.PrachiSingh, Student, MBA Final Year, Jagran Institute of Management, (Email id- prachi.jim.mba.2021@gmail.com)
[2]Mr. Kartikey Gupta, Student, MBA Final Year, Jagran Institute of Management, (Email id-kartikey.jim.mba.2021@gmail.com)
[3]Mr. Pawan Omer, Assistant Professor, Jagran Institute of Management, (pawan.omer@gmail.com)

Abstract
Usage of AI systems carries tremendous opportunities and threats of changes and even disappearance of certain professions. The power to re-design the management system in accordance with new opportunities and challenges will be a key factor in adapting organizations to the new conditions in the interests of workers, employers and society. This study includes the analysis of the synthetic Intelligence usage trends and its influence on the labour market and manager's job roles.
AI shown special tradition within the management of the compound system as well as the help for individuals in different kinds of processes. AI is one among the most frequently used in the business where it is used for the decision-making process support, making different quite the simulations as well as the base for the evolving competitive advantage of the association. Whit implementing the AI system in several departments in an organization there is a possibility to increase performances of the business processes as well as the increasing gratification whit the service or the merchandises that organizations consume.

Keywords: Artificial intelligence; competitive advantages; organisational performance.

Introduction

AI (Artificial Intelligence) is that the machines ability to perform intellectual functions as humans does such as perceiving, learning, reasoning, solving problems, designing etc. The benchmark for AI is that the human level concerning in terms of reasoning, speech and vision, problem solving.
The main goal of developing an AI system is to create a system that will be able to replace humans' beings in the context of the way of thinking and also creating alternatives for decision making. Furthermore, apart from substituting human beings, AI is additionally aimed at supporting decision making or analysing data in organizations. AI are often also related to the automated systems that have the possibility of thinking or have a significant level of intelligence based on which system can make decisions and adapt its behaviour regarding the characteristics of the environment.

AI Management and Organizations

AI Management and Organizations Artificial intelligence (AI) is re-envisioning the corporate ecosphere, enhancing innovation and productivity, and helping organizations think greater. Organizations can use AI to enhance their products, processes and decision-making. Using the

technology available today, organizations should be ready to achieve organizational agility powered by AI.

The impact of AI is being felt crossways all productions. There are multiple samples of implementing AI in the supply chain, transportation, education, operations, marketing, and just about every industry that's moving toward digitalization, and switching from manual activities to technology-assisted ones. With the assistance of AI, establishments are better well-appointed to fight calamities using AI decision-making algorithms, detect variances and predict imminent behaviour. AI enhances automation and reduces the human-intensive labour and monotony involved in forecasting and prediction analysis

.

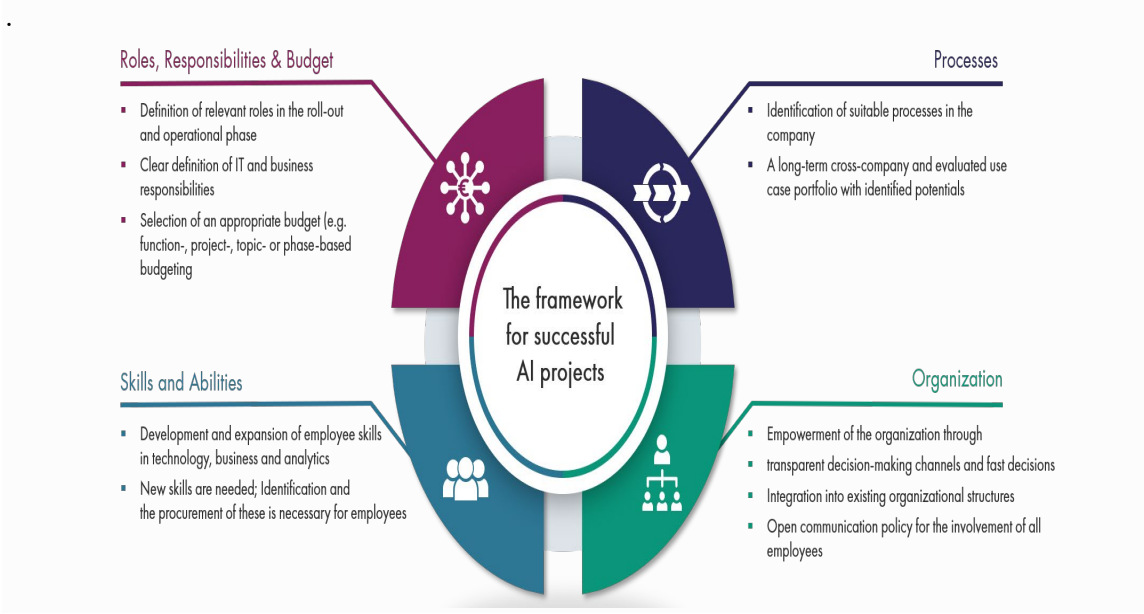


Fig 01-Googleimages.com

Organizations are categorized by their institutional properties including arrangement, size and enactment. These factors provide different contexts for the event and implementation of AI, and reflect the positive or negative consequences of the technology. Management plays a perilous role in pronouncing and associate the technology (e.g. through provision of resources), and should use it as a business strategy. AI isn't operational the same in all circumstances.

Artificial intelligence: - definition and its application

Introduction of AI (AI) is necessary to discuss its impact on business. Any sort of computer software that engages in humanlike happenings such as learning, planning, and problem-solving, is mentioned as "artificial intelligence." AI is usually viewed as a complement to human intelligence and ingenuity, instead of as anadditional.

The applications of AI in business are many, from improving associations with employees and customers to finding patterns in extreme data volume to performing repetitive tasks. These

should be an excellent benefit to most managers as it means they should have more time to focus on how they add value to their organization. The key's to embrace the opportunity artificial intelligence in business presents for separate and organization success, including scaling your skills and using AI to scale your impact.

Applications of Artificial Intelligence

1. Marketing:-

Your presentation meanings may already be using AI in various ways. It are often used to helping in develop marketing strategies, but it also can be used to execute them based on the customer's interests and preferences.

By analysing consumer behaviour supported data, AI tools also can abet in market research. All of those data-driven insights will help businesses evaluate their marketing campaigns and develop more effective plans for the future

2. Sales: -

However, AI can provide human professionals with the insights they have from time to time. When used properly, it can help improve sales functions generally, also as forecast trends and predict consumer behaviour.

Using AI to rise understand customer needs, sales tools can improve communication and coordination. This may allow sales professionals to better manage their time, identify who they need to follow up with and when and where customers may be ready to convert.

3. Research &Development: -

With its ability to gather and analyse massive amounts of information efficiently and accurately it can help us gain a deeper understanding of nearly any industry including healthcare and pharmaceuticals, financial, automotive, and more.

Machine learning and AI can help us solve problems we've never thought of before. However, AI also will lead to new discoveries and ways to improve products and services as well as accomplish tasks. In terms of strategy and effectiveness, AI aids in R&D activities.

4. Human Resource Management

Is there an area for machines in a business with the word "human" in its name? Indeed! Recruiting to talent management, AI has the potential to revolutionise a number of HR processes. Automating repetitive tasks can certainly improve efficiency and economize, but AI is capable of far more. Robot Vera was employed by PepsiCo to interview candidates for sales situations by phone.

Artificial Intelligence in business management:-

AI can help in all characteristics of business management, whether it's categorization of emails or responding swiftly. Intelligent assistants such as Siri and Google Now, smart devices, automated insight and security surveillance are all the perfect illustrations of how AI can be constructive.

The following are examples of how Artificial Intelligence can be used in business management:

- Spam filters
- Smart email categorisation
- Voice to text topographies
- Smart personal supporters, such as Siri, Cortana and Google Now
- Automated responders and online customer support
- Process automation System
- Sales and business forecasting Systems and Programming
- Security Surveillance System
- Smart Devices that adjust according to behaviour
- Automated insights, especially for data-driven industries (e.g. financial services or e-commerce)

Future of Artificial Intelligence in Business Management:-

"AI is as much a management challenge as it is a technical challenge"

Artificial intelligence (AI) technology mimics human intelligence to accomplish tasks on machines or organisations. Presently, AI practises include chatbots, smart assistants, manufacturing robots, and self-checkouts, among other routines.

According to research, by 2025, the AI market will be worth $169.41 billion. Industries that will have the ambition, this growth are IT & telecom, media & advertising, retail, healthcare, automotive & transportation, and Banking, Financial Services and Insurance (BFSI).

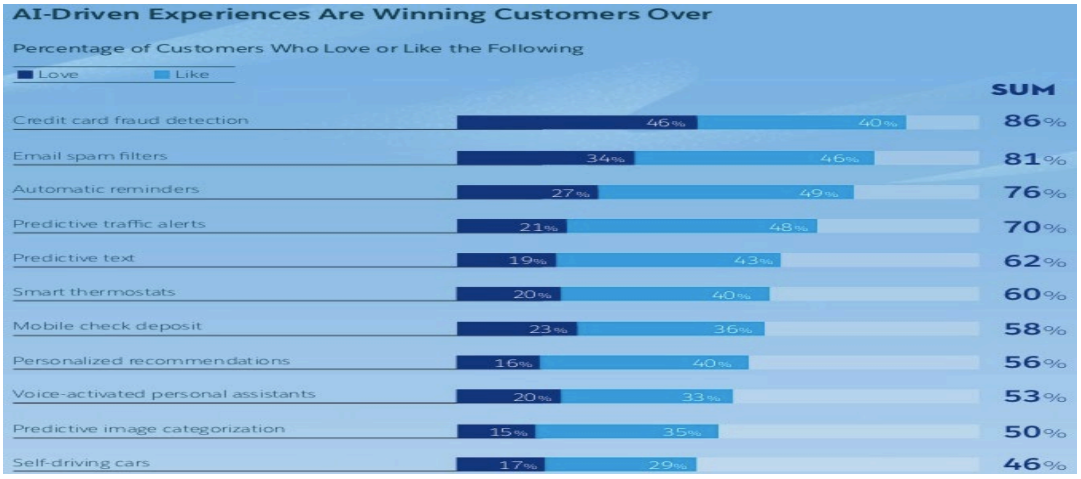


Fig 2 (Source-https://csuglobal.edu)

Conclusion:-

The use of artificial intelligence in business management is a comprehensive practice due to many benefits that this technology offers and an occasion to secure operational pedals. The opportunities of these algorithms are miscellaneous and include decision-making, strategic planning and other fields.

Among the undisputable advantages, one can pay attention to the measurement of AI use, its effortlessness of utilisation in multi-structured tasks, as well as chances to test the current presentation.

In the future, the compliance of this technology will become all pervasive due to the frequently evolving mechanisms for adaptation.AI systems and the opportunity of conjoining human efforts with machine manoeuvres.

Therefore, AI has already been functional to a whole host of authoritative processes, but there are hundreds or even thousands of additionalpresentations for virtually every segment of the contemporary economy.

What makes AI such a game-changing technology? The fact that it can accomplishanalogous tasks as human beings, but quicker, and with scarcer mistakes.

References:-

1- adovicMarkovic ,M. and Omolaja M ,(2009) ,‖INFORMATION MANAGEMENT-CONCEPTS, ANALYSIS AND APPLICATIONS, Himalaya Publishing ,Delji ,India.
2- DRIVE COMMUNICATIONS SUCCESS-The benefits of engaging traditional media and social media,CNW Group http://smr.newswire.ca/media/pdfs/whitepaper.pdf
3- https://csuglobal.edu/blog/why-ai-important
4- https://csuglobal.edu/blog/why-ai-important
5- International Development Research Centre,(1996) ,available in the internet http://www.fao.org/docrep/w6840e/w6840e02.html

Significance of White box testing and its approach

[1]AdarshSrivastava, Assistant Professor (MCA Dept.), Jagran Institute of Management,Kanpur,
E-mail_id:adarsh.srivastava1984@gmail.com
[2]Ashish Mishra, Assistant Professor (MCA Dept.), Jagran Institute of Management,Kanpur
E-mail_id:kanpur.ashish@gmail.com

Abstract:
Present day white box testing is very important in to today's software business to raise software quality. Both time and personnel are significantly reduced by it. Software sectors regularly use the numerous software testing tools that are readily available on the market to create high-quality software. White box testing in the software industry is crucial to raising software quality. Both time and personnel are significantly reduced by it. Software sectors regularly use the numerous software testing tools that are readily available on the market to create high quality.
Keywords: software quality ,Testing, Software sectors , Code, Technique etc.

White Box Testing

The "white box testing" method examines the program's design and generates test data from the program's logic and code. Glass box testing is also known as clear box testing, open box testing, logic driven testing, path driven testing, and structural testing..

White Box Testing Techniques:

Statement Coverage - With this technique, all programming statements are tested as much as possible.

• **Branch Coverage -** Using this technique, a sequence of tests are run to guarantee that each branch is tested at least once.

• **Path Coverage -** This technique entails testing every path that could exist, which means that every statement and branch are tested.

Static Testing

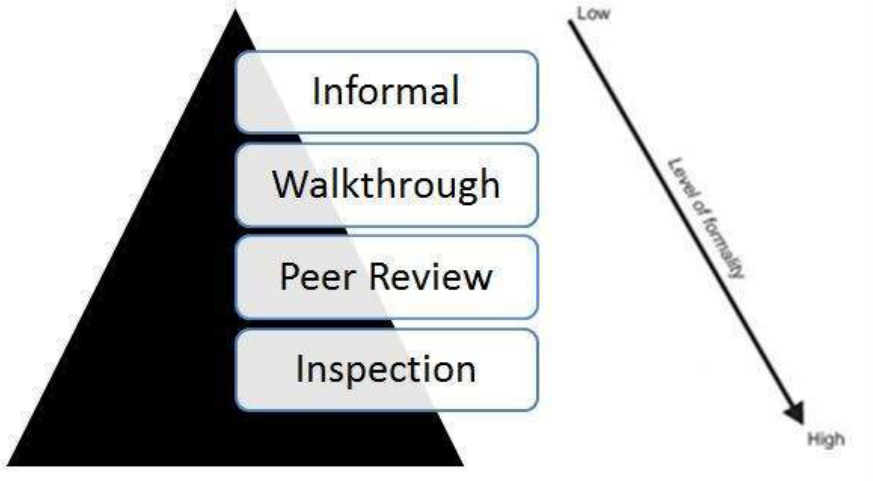
Static testing is a software testing technique that involves testing the software without running the code. It is divided into two parts, which are listed below:

- Review - This technique is frequently used to identify and get rid of mistakes or ambiguities in documents like requirements, designs, test cases, etc.

- Static analysis - Static analysis - The code written by developers is inspected for structural problems that may lead to defects (typically by tools).

Types of Reviews:

- The types of reviews can be given by a simple diagram:



Structural Testing

- Structural testing, also referred to as glass box or white box testing, is a technique where tests are created based on an understanding of the design or implementation of the software.
- Other names for structural testing include clear box testing, open box testing, logic driven testing, and path driven testing.
- **Structural Testing Techniques:**

➢ Statement Coverage is a structural testing technique that aims to test every programming statement with a minimum number of tests.

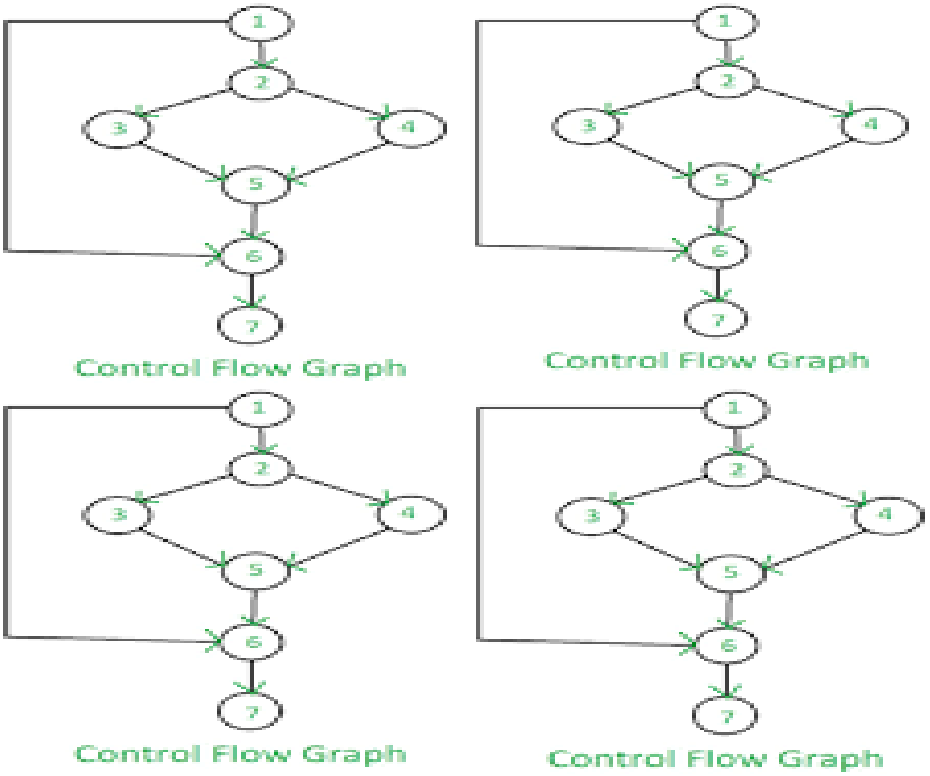
➢ Branch Coverage - Using this technique, a sequence of tests are run to guarantee that each branch is tested at least once.

➢ Path Coverage - This method entails testing every path that could exist, which means that every statement and branch are tested.

Code Functional Testing

Functional testing is a sort of software testing that involves testing the system against functional requirements and specifications. Functional testing verifies that the application satisfies the requirements or specifications. This testing is unconcerned about the application's source code.

The control flow graph of a program



The graphical depiction of control flow or computation during the execution of programs or applications is called a control flow graph (CFG). Since control flow graphs may precisely depict the flow inside a program unit, they are frequently utilized in static analysis as well as compiler applications.

Black box Testing

Black-box testing is a type of software testing that checks an application's functioning based on requirements. It is often referred to as specifications-based testing. This type of testing is typically performed by an Independent Testing Team within the software testing life cycle.

This test approach is applicable to all levels of software testing, including unit, integration, system, and acceptability testing.

Behavioral Testing Techniques:

The Black Box testing process uses a variety of methods

- Equivalence Class
- Boundary Value Analysis
- Domain Tests
- Orthogonal Arrays
- Decision Tables
- State Models
- Exploratory Testing
- All-pairs testing

Random Testing

Random testing, sometimes known as monkey testing, is a type of functional black box testing that is used when there is insufficient time to design and execute tests..

Random Testing Characteristics:

• Random testing is used when problems are not found at regular periods.
• The system's dependability and performance are tested using random input.
• Saves time and effort compared to actual testing efforts.
• Other testing methods are ineffective.

Random Testing Steps:

- Random inputs are found and tested against the system.
- Test inputs are chosen independently of the test domain.
- Random inputs are used to execute tests.
- Keep track of the results and compare them to the projected outcomes.
- Reproduce/replicate the problem and report any faults, then correct and retest.

Requirements based Testing

Requirements-based testing is a testing method that derives test cases, conditions, and data from requirements. It comprises functional assessments as well as non-functional qualities like performance, dependability, and usability.

Stages in Requirements based Testing:

• **Specifying Test Completion Criteria -** Only after all Functional and Non-Functional Testing is Complete, is Testing Complete.
• **Create test cases using five parameters:** the initial condition, data setup, inputs, anticipated results, and actual results.
• **Run Tests -** Run the test cases against the system being tested, then record the outcomes.

• Check the test results to make sure they line up with what was anticipated.

• Check Test Coverage - Check to see if both functional and non-functional components of the requirement are covered by the tests.

• Track and Manage Defects - Any flaws found during testing are tracked through the defect life cycle and fixed. We can determine the overall condition of the project by looking at the defect statistics that are kept.

Requirements testing process:

- Testing must be completed in a timely way.
- Testing process must be effective in order to contribute value to the software life cycle.
- Exhaustive testing of the system is impossible, the testing procedure must also be efficient.
- Testing must provide an overall state of the project, it must be manageable

References

- "The Complete Guide to Software Testing – Second Edition," Hetzel, B.
- "The Art of Software Testing," Myers, G. J., Wiley, John, New York, 1979.Google Scholar.
- "PRINCE 2: Project Management for Business," 4th edition, CCTA, 1996. ...
- "British Library Testing Course," Ref: P6188A/T0, AMSL, 1997.

The study of Brand Management

[1]Dr. Akshat Gupta, Department of Business Administration, Jagran Institute of Management Kanpur 208014, India
Email: akshatjim7@gmail.com
[2]Ms.Prachi Singh, Student, MBA Final Year, Jagran Institute of Management, (prachi.jim.mba.2021@gmail.com)

Abstract
A brand is defined as a consistent and clearly stated promise to deliver unique, focused and relevant benefit that differentiates an offering from those competitors. The function of branding is to create preference by managing consumer's awareness and expectations of the brand. This is accomplished by developing a brand strategy that outlines rules and guidelines to ensure that the brand owner's goals and objectives are met. The role of branding has become the integral part of business strategy as it defines a realistic and manageable brand promise, dealing what the brand owner must deliver as what consumers expect of the brand.
The primary interest in choosing this area of study is to gain more information about the current trends related to the topic. Perception can be created in the mind of target markets if the brand is effectively managed. Branding is creating that right perception. The perception of the target market has to be analysed and that has to be adjusted with the companies positioning statements so that perceptions match. This enjoys higher brand equity in the market place.
Key word: brand management, brand equity

Introduction

Brand management in marketing, defined as t perceived value of any brand regarding its product or its product line or brand over time. Effective brand management helps to increase the customer loyalty towards brand and also helps to increase its customer base. Brand management is also helps to grow company in positive aspects in market its creates as its brand value over a period. Brand management begins with an analysis on how a brand is currently perceived in the market, proceeding to planning how the brand should be perceived if it is to achieve its objectives and continues with ensuring that the brand is perceived as planned and secures its objectives.
Brand managers are responsible for **overseeing any aspect of marketing that has to do with a company's brand, and ensuring that all branding decisions ultimately result in stronger sales**. To achieve that alignment, brand managers tend to work with multiple areas of marketing, like research, content, social, and design. Brand management is broad term used to describe brand values in the market strategies to maintain, improve and bring awareness to the wider value and reputation of a brand. **Brand management** includes managing the tangible and intangible characteristics of brand. It means defining the brand, positioning the brand, and

delivering. **Brand management** is a group of activities that companies use to create, nurture and promote their brand to potential customers.

Objectives

Brand management is effective as well as crucial process of developing and continuously improving with current scenario of time as time changes the management of brand and its values also changes and on the basis of this there are certain objectives but not consider as limited:

- Create a strong brand identity.
- Raise brand awareness.
- Establish brand positioning.
- Tell a compelling brand story.
- Develop customer loyalty.

Need of brand management in market

When you think of brands, which ones come to mind? Coca-Cola, Starbucks, McDonald's, Walmart, Apple, Nike. Millions of brands populate our world, but the true test of their longevity and resilience is brand management. Without brand management, none of these brands could have achieved the lasting success they have.

Every marketer knows that brand management is extremely important. After all, the strength of your brand is dependent on customer perception. But influencing how you're perceived in the market is extremely complicated, and unfortunately, there's no magic formula or quick fixes for earning customer loyalty.

To build a brand that customers choose over competitors takes dedication and hard work. It starts with a clearly defined brand vision, organizational self-reflection, and company-wide discipline. Easy to say, harder to execute. But having a solid understanding of the components of brand management will help you get there.

Brand managers work **to ensure that both aesthetic and intangible aspects of a brand align**. This includes packaging, product or service quality, marketing campaigns, and the customers' emotional experience of interacting with your brand.

Four reasons why brand management is important to marketers

Brand management should be top of mind for everyone at an organization but it's usually marketers that are leading the charge. That's because superior brand management makes their job much easier! While the benefits of brand management are vast and wide reaching, these four tend to top the list for marketers.

1. Improved brand perception

Brand management and brand consistency go hand in hand, which is good because they're pillars of a strong brand perception. When brands present a consistent customer experience across channels, it builds customer trust. Shoppers know that they can count on this brand to meet their needs. For marketers, brand management allows them to drive brand perception bydelivering this experience time and time again.

2. Workflow efficiencies

As Omni becomes common practice, being able to deliver a consistent experience across channels increases in difficulty as well. Having processes in place to support brand management is not only beneficial to the customer but also to the teams behind the scenes. Developing a strong brand identity that marketers can follow eliminates bottlenecks in the process that arise alongside confusion. Understanding your brand management process also makes it easier to see opportunities for improvement, including system integrations and automation options.

3. Content optimization and reuse opportunities

A lot of time, money, and effort goes into creating content, but many teams aren't getting everything they could from their investments. Understanding how and where your content is being used will provide insights into how it can be optimized, repurposed, or reused. Extending

the life of your content and leveraging learning from past projects increase efficiencies and help teams deliver the content customers desire.

4. A safe and secure brand

If you're building a brand, you want to ensure that you have control over how and where your brand assets and elements are being used. Leveraging tools like a DAM solution, along with digital rights management (DRM) technology, keeps content safe and secure — as well as easy to access and share. As a marketer, knowing that your brand guidelines are automatically enforced via a strong previsioning structure gives you the peace of mind needed to clear the way for other more meaningful work.

RATIONALE:-

MEASURING BRAND EQUITY

In recognition of the value of brands as intangible assets, increased emphasis has been placed on understanding how to build measure, and manage brand equity. There are three principal and distinct perspectives that have been taken by academics to study brand equity.

Customer based.

From the customer's point of view, brand equity is part of the attraction to, or repulsion from a particular product from a particular company generated by the "non objective" part of the product offering, i.e., not by the product attributes per se. While initially a brand may be synonymous with the product it makes, over time through advertising, usage experience, and other activities and influences it can develop a series of attachments and associations that exist over and beyond the objective product. Importantly, brand equity can be built on attributes that have no inherent value.

Company based

From the company's point of view, a strong brand serves many purposes, including making advertising and promotion more effective, helping secure distribution, insulating a product from competition, and facilitating growth and expansion into other product categories. Brand equity from the company perspective is therefore the additional value (i.e., discounted cash flow) that accrues to a firm because of the presence of the brand name that would not accrue to an equivalent unbranded product. In economic terms, brand equity can be seen as the degree of "market inefficiency" that the firm is able to capture with its brands.

Financial based

From a financial market's point of view, brands are assets that, like plant and equipment, can and frequently are bought and sold. The financial worth of a brand is therefore the price it brings or could bring in the financial market. Presumably this price reflects expectations about the discounted value of future cash flows. In the absence of a market transaction, it can be estimated, albeit with great difficulty from the cost needed to establish a brand with equivalent strength or as a residual in the model of the value of a firm's assets.

Comprehensive models of brand equity have been developed in recent years to incorporate multiple perspectives Each of the three brand-equity measurement perspectives has produced relevant work.

Limitations of branding:-

Cost

If you wish to create and maintain a strong brand presence, it can involve a lot of design and marketing costs. A strong brand is memorable, but people still need to be exposed to it, this often requires a lot of advertising and PR over a long period of time, which can be very costly.
There are also costs involved with the creating of a brand image or logo (Paying for a designer, printing new letterheads/business cards etc.), and although most of these are only one off costs, they are still relatively large for most small businesses.

Impersonal

One of the main problems with many branded businesses is that they lose their personal image. The ability to deal on a personal basis with customers is one of the biggest advantages small business have, and poorly designed branding could give customers the impression that your business is losing its personal touch.

Fixed Image

Every brand has a certain image to potential customers, and part of that image is about what products or services you sell. If you are known for selling just one product, and you want to sell another product, will you be able to do so effectively ? If you sell computers, would your brand name be suitable for selling vacuum cleaners? If your brand is focused too strongly on one product, it can limit your ability to sell other products.

Timescale

The process of creating a brand will usually take a long period of time. As well as creating a brand and updating your signs and equipment (e.g. Stationary, vehicles etc…), you need to expose it to your potential customers. It is commonly shown that people need to see an advert at least three times before they absorb it, which means you will need to advertise and promote the brand for a considerable amount of time before it will become well known.

Conclusions

Therefore it can be said that the clear the concept of a product or service is to the audience the better it is for its brand value. The importance of brand management is listed in the following points- First; Brands help recognize the Product or Service. Second, Brand Management Helps Identify the Audience. Third, Brand Management helps to build a sense of loyalty among the employees. Fourth, Brand Management helps in safeguarding the brand. Fifth, Brand management helps to create a positive perception and measure the brand's perception. Students who face difficulty in understanding the concept of brand management can take the help

of instant assignment writers from SourceEssay to clear their doubts and submit high quality flawless and non-plagiarized assignments on brand management.

Reference

Lim, W. M., Jee, T. W., & De Run, E. C. (2020). Strategic brand management for higher education institutions with graduate degree programs: empirical insights from the higher education marketing mix. *Journal of Strategic Marketing*, *28*(3), 225-245.

Wiedmann, K. P., Hennigs, N., Schmidt, S., &Wuestefeld, T. (2011).The importance of brand heritage as a key performance driver in marketing management. *Journal of Brand* Management, *19*(3), 182-194.

Almeida, Paul, and Bruce Kogut (1999), "Localization of Knowledge and the Mobility of Engineers in Regional Networks," Management Science, 45 (7), 905-917.

Amit, Raphael and Birger Wernerfelt (1990), "Why Do Firms Reduce Business Risk?," The Academy of Management Journal, 33 (3), 520–33.

Andrews, Rick L., and Imran S. Currim (2003), "Retention of Latent Segments in RegressionBased Marketing Models," International Journal of Research in Marketing, 20 (4), 315-321.

Argote, Linda, and Ella Miron-Spektor (2011), "Organizational Learning: From Experience to Knowledge," Organization Science, 22(5), 1123-1137.

Belliveau, Maura A., Charles A. O'Reilly, and James B. Wade (1996), "Social capital at the top: Effects of social similarity and status on CEO compensation," Academy of management Journal, 39 (6), 1568-1593. Bertrand, Marianne (2009), "CEOs," Annual Review of Economics, 1 (1), 121–50.

Boeker, Warren (1997), "Executive Migration and Strategic Change: The Effect of Top Manager Movement on Product-Market Entry," Administrative Science Quarterly, 42 (2), 213-36.

Bolton, Patrick, Hui Chen, and Neng Wang (2011), "A Unified Theory of Tobin's q, Corporate Investment, Financing, and Risk Management," Journal of Finance, 66 (5), 1545-1578.

Boulding, William, and Richard Staelin (1995), "Identifying Generalizable Effects of Strategic Actions on Firm Performance: The Case of Demand-Side Returns to R&D Spending," Marketing Science, 14(3), 222-236.

Bourdieu, Pierre (1985), "The Forms of Capital," in Handbook of Theory and Research for the Sociology of Education, J.G. Richardson, ed. New York: Greenwood, 241–258. Boyd, Eric D., Rajesh Chandy, and Marcus Cunha Jr. (2010) "When Do Chief Marketing Officers Impact Value? A Customer Power Explanation," Journal of Marketing Research, 47(6), 1162-1176.

Burt, Ronald S. (1992), Structural Holes: The Social Structure of Competition. Cambridge, MA: Harvard University Press. _____ (2000), "The Network Structure of Social Capital," in Research in Organizational Behavior, B. M. Staw and R. I. Sutton, eds. Amsterdam, London and New York: Elsevier Science, 345-423.

Instructions for Authors

MANUSCRIPT STYLE

Manuscripts should be submitted in MS-Word format and typed in Times New Roman 12-point font. The submitted MS-Word file must be named as 'title of the paper'. Authors' names or identity should not display in the file name or in 'Properties' of the file. They must be single spaced (including references, appendices, tables, and figures). As reviewers often prefer to write notes on the manuscript, authors should use one inch (2.54 centimeters) margins. Every page in the manuscript should contain a short running head and the page number. Manuscript must be formatted as Justified. Pages should measure 8.5 by 11 inches. Manuscript length should be limited to 12 pages inclusive of references, appendices, tables and figures.

MAJOR SECTIONS OF THE PAPER

TITLE PAGE

Title page must include the title of the paper (not more than 15 words), authors' name(s), affiliation, email id and phone number. Other than title page, authors' name(s), affiliation, email id and phone number should not appear anywhere else in the paper.

MAIN DOCUMENT

The principle divisions of the manuscript should appear in the following order: body of the article (Abstract, Keywords, Introduction, Literature Review, Research Methodology, Analysis, Findings, Conclusion etc.), references and appendices. Abstract (limit 250 words) should be included in the main document of the manuscript. There must be title of the paper at the top of this page. Footnotes, tables and figures must be numbered with short description and must be placed within manuscript. The body of the article begins immediately on page 1. The title of the paper should appear at the top of this first page. It should be centered, bold-faced, and in all capital letters. Number all pages, including those with references.

HEADINGS

Main headings should be used to designate the major sections of an article. Within the main body of the paper, the major headings typically include such things as INTRODUCTION, METHOD, RESULTS, and DISCUSSION. Supporting material, such as references and appendices are also treated as major headings. In all cases, major headings should be left-aligned, bold-faced and typed in all capital letters. Secondary headings should be typed with the left margin, in title case (small letters with major words beginning with capitals), and in bold.

TABLES AND FIGURES

Number tables and figures consecutively (one series for tables, one for figures) from the beginning to the end of the article. Indicate the position of each in the text.

CITATIONS

Giving proper credit to the sources of original ideas and previous work is an important aspect of good scholarship. Inappropriate or inaccurate citations do not do justice to the authors cited and can be misleading to readers. Citations must be in alphabetical order.

Example: Several studies (Ferris & Kacmar, 1992; Malhotra & Bazerman, 2008; Morrison, 1993a, 1993b) support this conclusion.

Also note that two or more works by the same author (or by an identical group of authors) published in the same year are distinguished by "a," "b," etc., added after the year. If a work has two authors, give both names every time the work is cited in the text. If a work has more than two authors, use "et al." after mentioning the name of first author.

Example : Emotional exhaustion is related to work attitudes (Cropanzano and Byrne, 2003).

.. exhaustion was also related to job performance (Adams et al., 2008). (For more than 2 authors)

REFERENCES

References must be in APA style.

Examples:

Goggin, W. C. (1974). How the multi-dimensional structure works at Dow Corning. Harvard Business Review, 55(1): 54-65.

Katz, D. and Kahn, R. L. (1978). The social psychology of organizations (2nd ed.). New York: Wiley.

Duncan, R. G. (1971). Multiple decision-making structures in adapting to environmental uncertainty. Working paper no. 54-71, Northwestern University Graduate School of Management, Evanston, IL.

Wall, J. P. (1983). Work correlates of the career plateau. Paper presented at the annual meeting of the Academy of Management, Dallas, TX.

Smith, M. H. (1980). A multidimensional approach to individual differences in empathy. Unpublished doctoral dissertation, University of Texas, Austin.

APPENDICES

The appendices present lengthy but essential methodological details, such as explanations of the calculation of measures or items in a new survey instruments. Presentation should be concise but not abbreviated. Each appendix should be treated as a major heading. The title of each appendix should be typed in all capital letters, centered, and bold-faced. Multiple appendices are APPENDIX A, APPENDIX B, etc. A single appendix does not require a letter.

JAGRAN EDUCATION FOUNDATION

Under the aegis of Shri Puranchandra Gupta Smarak Trust established in 1987

Jagran

"An Initiative of Dainik Jagarn"

Jagran Education Foundation, was established under the aegis of Shri Puranchandra Gupta Smarak Trust as an educational initiative of Jagran group, is running successfully and becoming the centre of quality education. JEF works on the philosophy of 'Education for All'.

Jagran Institute of Management, established in the year 2006 is the most mordern purpose built business school of Uttar Pradesh. It is equipped with state of art facility that promotes experiential learning, where students are mentored by an expert team of faculties, supported by rich library of books, academic journals and magazines. The Institute provides 2 years full time Master of Business Administration (MBA) and 2 years full time Master of Computer Application (MCA) Program duly affiliated to Dr. APJ Abdul Kalam Technical University, Lucknow.

The pedagogy of the institute includes holistic development of the students along with enhancing their employability skills by organizing various international & national conferences, symposiums, seminars, guest lectures, workshops and industrial visits. These help students to leverage their enhanced leadership and to build sustainable advantage for their workplace and become responsible citizens of the nation.