VOL 1 | MAY 2024

Bytebeat

UNRAVELING THE WONDERS OF COMPUTING"

DEPARTMENT OF COMPUTER SCIENCE

DUM DUM MOTIJHEEL COLLEGE

List of Editors

PROF. (DR.) SUBHRANIL SOM
Principal
Bhairab Ganguly College

DR. TUHIN UTSAB PAUL
Associate Professor and HoD
St. Xavier's University, Kolkata

MR PARTHA SARATHI GUPTA
Assistant Teacher
Dighalgram Netaji Vidyapith
High School

DR. MUNMUN BISWAS
Assistant Professor and HoD
Brahmananda Keshab Chandra
College

SIMERJEET SINGH BEDI
2nd year Student
Department of Computer Science
Dum Dum Motijheel College

ANANTA PANDIT
2nd year Student
Department of Computer Science
Dum Dum Motijheel College

RAJA DAS
2nd year Student
Department of Computer Science
Dum Dum Motijheel College

The Telegraph online
edugraph
Digital Media Partner

Principal Message

Dear Readers,

It's a proud moment for us that our students of Computer Science Department are gearing up to bring the first edition of Departmental Magazine "Bytebeat". This Initiative will not only foster Innovation and creativity in the students but will also create an environment of technological advancements in the global scenario.

Needless to mention Computer Science is a field with evolving technologies, the students would be updated with the advanced write ups in cutting edge technologies and advancements in technologies especially in the field of Computer Sciences in the magazine "Bytebeat". Our magazine will help it in doing so.

I would like to thank the Magazine Committee comprising faculty members and students. The efforts of all of them is very valuable for creation of this magazine.

I hope the readers of the magazine will find insightful and thought provocating articles in it and would enjoy in reading it.

Warm Regards

Dr. Pradeepta Gupta Roy

Principal

Dum Dum Motijheel College

HOD Message

Dear Faculty, Staff, Students, and Alumni,
It is with great pleasure and pride that I address you all in this edition of our departmental magazine. As we reflect on the achievements and milestones of the past year, I am filled with a deep sense of gratitude for the remarkable individuals who make up our vibrant community.

Our department continues to thrive, driven by a relentless pursuit of excellence in teaching and service. The contributions of our faculty, students, and alumni have left an indelible mark on the field of computer science.
I would like to extend my heartfelt appreciation to our dedicated faculty members for their unwavering commitment to academic rigor and intellectual inquiry. Your passion for teaching and mentorship inspires our students to reach new heights and pursue their dreams with confidence.

To our students, I commend your relentless pursuit of knowledge and your eagerness to embrace new opportunities. Your curiosity, creativity, and determination are the driving forces behind our department's continued success, and I have no doubt that you will go on to accomplish great things in your future endeavors.

I also want to express my gratitude to our staff members for their tireless efforts behind the scenes, ensuring the smooth operation of our department and providing invaluable support to faculty and students alike.

As we look ahead to the future, let us remain steadfast in our commitment to innovation,
collaboration, and inclusivity. Together, we will continue to push the boundaries of what is possible,

advancing the frontiers of computer science and making a positive impact on society.
I invite each and every one of you to join me in celebrating our collective achievements and inembracing the exciting opportunities that lie ahead. Together, we will shape the future of computer science and inspire generations to come.
Warm regards,

Lt. Debi Prasad Bhattacharya
Head of the Department of Computer Science

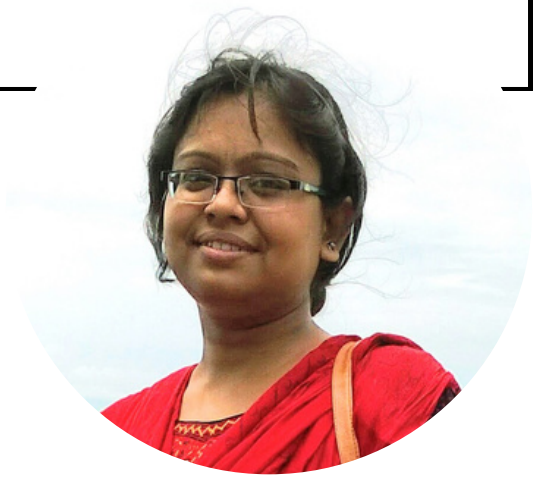
Amrita Ma'am message

It is indeed a proud moment for our Computer Science Department as our students have taken the initiative to release the annual magazine "Bytebeat". I would like to remember a very famous quote of Swami Vivekananda – "If you think yourselves strong, strong you will be". We hope that the constant effort of our students to push their boundaries will make them stronger and boost their self confidence. Through this message, I wish them all the very best.

Dr. Amrita Roy Chowdhury
Assistant Professor
Department of Computer Science
Dum Dum Motijheel College

Anasua Ma'am message

An educational institution is like the second home to the learners. In Computer Science department of Dumdum Motijheel College also, we, the faculties and the students come to learn together. A departmental magazine is the reflection of how students are learning... finding interest in the subject , gathering knowledge , exploring new topics and moreover learning to work in a team structure. In my note of encouragement I wish them success for the upcoming event and awaiting many more yet to come.



President message

Dear readers,

I am Excited for reflecting my thoughts on the First Volume of our Computer Science Magazine. As we all are from diverse Backgrounds which brings new experiences every day in our campus.

The journey of making this magazine was not simple . I initiated to work upon this idea with the support of our esteemed faculty members.

Our excellent team had done months of hard work to bring to you diverse range of articles about the cutting edge technologies and recent breakthroughs in computer science. I extend my sincerest gratitude to my Design team, Research team and Content Team who were the important pillars for creation of this magazine.

I hope you find this magazine insightful and thank you all for your support.

Warm Regards ,

Simerjeet Singh Bedi

President

Magazine committee

Department of Computer Science

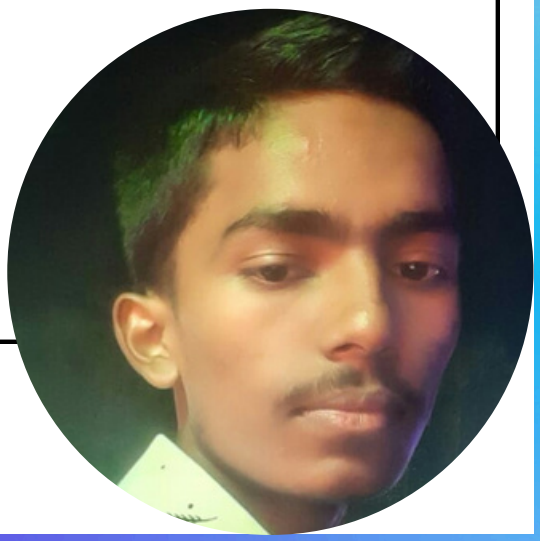
Dum Dum Motijheel College

Vice President message

Any impossible journey is done by teamwork!

In the beginning, i was worried when DUM DUM MOTIJHEEL COLLEGE computer science department announced for releasing annual magazine.But in the same time i was also very hopeful.
I can clearly recall my start of this extremely beautiful journey of being a part of the department of the computer science. Having a memory of how it all started.
We operated both in online and offline mode,what remained common irrespective of the mode of events was the enthusiastic participation of the department members. We spent some memorable moments together in this journey and i was also glad to joy.
I feel proud that with eagerness of the department's faculty. Students and department members were contributed enormously in the process and as a result i see the department to reach a new landmark.

With loads of smiles,
Ananta Pandit
Vice President
Magazine Committee
Department of Computer Science
Dum Dum Motijheel College



Design Team message

Dear Readers;

As the part of design team, we are excited to share with you our department's first volume of magazine "BYTEBEAT". We hope you Really enjoy reading and learning from this magazine.

Our journey starts from being member of this excellent design team to having our orientation session with faculty members and President and Vice President.

The faculty members were very supportive as they helped us every time to answer our silly doubts to supporting us in tough situations. We want to thank them for their support.

The Role of President and Vice President was also very appreciable as they have several meetings with us and they always remain with us to create quality designs for the magazine.

This is our first edition of the magazine and we have included creative design elements in it to make it a stunning magazine.

And also without the support and collaboration of all the other teams Doing this was not even possible.

We hope you enjoy reading this magazine and love our designs too.

Warm Regards,

Design Team,

Magazine committee,

Department of Computer Science,

Dum Dum Motijheel College

Content Team message

Hello Readers,

This is a little message from content team, we are really exited to present this magazine to you. First, we would like to thank our Faculty members, our President and Vice-President for helping us make the best and most suitable content for the readers, through several online meetings and offline sessions. We have taken help from a lot of articles, data available online and books and even other Magazines to make the content accurate and informative.

We would like to thank our Research team to provide us with proper materials, information to make the content upon and our Design team for making our content look beautiful and presentable to your eyes.

At last we would like to thank you Readers for choosing to read this magazine. We hope you find the content enjoyable and engaging.

Take our regards,

Content Team,

Magazine Committee,

Department of Computer Science,

Research Team message

We hope this message finds you well. We are writing to you on behalf of the research team for the computer science magazine of DUM DUM MOTIJHEEL COLLEGE. First, we would like to thank our faculty members, our President and Vice-President for encourage ourselves.

In ghe beginning of the journey of making this magazine was not easy. We are started to work with the help of our respective faculty members. Our main goals to research about cutting edge technologies and their major points and give it to content team. Day by day this journey brings new experiences to us.

We would like to take this opportunity to thank you for your loyalty and support of our publication. We wish our computer science department to reach new milestone through this magazine.

Best regards,

The Research Team

Magazine Committee,

Department of Computer Science,

Dum Dum Motijheel College

Contents of Articles

SQL Injection Attacks: Mode, Detection and Prevention

By- Prof. (Dr.) Subhranil Som
Principal
Bhairab Ganguly College

SQL Injection (SQLI) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. This can allow an attacker to view data that they are not normally able to retrieve. This might include data that belongs to other users, or any other data that the application can access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior. In some situations, an attacker can escalate a SQL injection attack to compromise the underlying server or other back-end infrastructure. It can also enable them to perform denial-of-service attacks. Web applications are presently utilized for online administrations, for example, long-range informal communication, shopping, managing accounts, and so forth. Web applications deal with complex user information. Unauthorized access can lead to the collapse of a system; it can even harass the existence of a company, a bank, or a branch. SQL Injection Attacks (SQLIA) are a standout among the most hazardous security dangers to web applications. Researchers are working to control SQLIA at the application layer, but beforehand they are trying to prevent SQLIA at the database level through stored procedures. This article shows ways to prevent SQLIA in stored procedures. The application is secured from attacks with the technology in two phases because if the first phase is unable to protect, then the second phase can prevent attacks.

Introduction

SQL injection exposures have been communicated as being greatly unsafe for the database. Vital databases are absolutely accessible to attackers by injecting SQL queries that are retrieved by web applications. As customer information is frequently kept in these databases, important information is lost, resulting in a security breach. Attackers can even use SQL injection exposure to control and make the web application structure worse. A class of code-injection attacks is pointed to by SQL injection; the customer gives the data that is incorporated into a SQL query in such a way that part of the customer's information is known by SQL codes. SQL commands given by attackers right away to the database through these vulnerabilities. These attacks are dangerous to any Web application that gets data from customers and goes along with it into a SQL request to a key database.

Types of SQLIA

Tautologies

These kinds of attacks inject SQL tokens into the conditional query statements, which are constantly assessed to be genuine. This type of attack uses the WHERE clause to extract the valuable information from the input fields, which are easily accessible, which leads to the failed authenticity of control. Illustration 1: Think about a web application that collects info through Customer, by means of the above SQL query, The aftereffect is as follows:

Assume an attacker gives a name like this:
SELECT * FROM Customer WHERE name = 'ritu' OR '1' = '1

This statement will give back all lines from the database of customer, instead of 'ritu' is a genuine customer name or not since OR is added to the WHERE clause. The result of '1' = '1 comparison will always be 'true', and the resultant of The WHERE clause assesses for all columns in the table to be genuine. On the off chance that this is utilized for validation, purposes, the attacker will frequently login as a first or last customer at the table.

Logically Incorrect Queries

At the point when a query is not required, an incorrect text from the database, including the required data, is returned. These Incorrect texts help attackers find parameters in the application and, in this manner, the application's database. Without a doubt attackers garbage info or SQL token injected into query language structure mistake, to deliver logical error, syntax error, or type mismatches purposefully.

Union Query

By using this strategy, the attacker provides the incorrect data with the few correct fields, the SQL query is sent with the 'Union' of both correct and incorrect fields. As a result, the dataset from the database is fetched with the correct fields.

.

Illustration 4:
An attacker could inject the text "' UNION SELECT Card_No from Credit_Cards where Acct_No=12450 --" into the login field, which produces the following query:

SELECT acc_inf FROM clients WHERE login='' UNION SELECT Card_No FROM Credit_Cards WHERE acct_No=12450 -- AND pass='' AND pin=

In the first statement, the login is null; hence, the query is invalid, while the other query fetches the result. In the current situation, the field "Card_No" will fetch out for Acc_No="12450". The consequences of the two queries are joined and returned as the output, which will show the Acct_No corresponds to the credit card.

Piggy-backed Queries
In this sort of attack, with the existing query, an attacker adds on extra queries, and with this type of query, the attacker doesn't change the original query but rather puts on a new query. with the old one resulting in multiple SQL queries received by the database. Initially, the existing query is implemented and the substitute query follows the already-implemented query. This sort of attack can be exceptionally unsafe. In the event that is effective, attackers can embed SQL queries of basically any sort in substitute queries, including stored procedures and Along with the first query they executed. This sort of attack is regularly reliant on database designs that contain many queries in one string is the weakness.

Illustration 3: In the event that the input is provided by an attacker " '; DROP TABLE client" in the 'pass' field application produces the query:

SELECT Acc_No FROM client WHERE login = 'ritu' AND pass = ';' DROP TABLE client -- 'AND pin = 321
After going through the first SQL query and detecting the delimiter (";") injected query is executed automatically by the database. which results in losing the client's useful information.

Stored Procedure

In this process, attackers pay attention to the stored procedures that are available in the database system. A database engine helps in the working of stored procedures. A stored procedure is just a piece of code that is exploitable. The stored procedure gives true or false values for the authorized or unauthorized clients. For SQLIA, attackers will write "; SHUTDOWN; --" with a login or secret key. The below query will be produced by the stored procedure:

Illustration 5:

SELECT cc FROM client WHERE Login= '1231' AND Pass='9999 '; SHUTDOWN;--;

It works like a piggyback attack. Firstly, the existing query is processed, subsequently followed by the other query, gets implemented and leads to the shutting down of the database. This states that along with the web application code, Stored procedure codes are equally exploitable.

Mode of SQLIA

SQL injection attacks can occur through various modes, each targeting different vulnerabilities in web applications or database systems. Some common modes of SQL injection attacks are given below:

In-band SQL Injection (Classic SQL Injection):

- **Error-based SQL Injection: Exploits error messages generated by the database to extract information about the structure of the database or the results of SQL queries.**
- **Union-based SQL Injection: Injects SQL UNION statements into input fields to combine the results of two SQL queries and retrieve additional information from the database.**
- **Boolean-based SQL Injection: Uses Boolean logic to infer information from the database by observing changes in the application's response based on true/false conditions.**

Out-of-Band (OOB) SQL Injection:

- Exploiting DNS: Utilizes SQL injection payloads to trigger DNS requests from the database server, allowing attackers to exfiltrate data or execute commands through DNS requests.
- Exploiting External Services: Injects SQL payloads that trigger interactions with external services controlled by the attacker, such as HTTP requests to a server under their control.

Blind SQL Injection:

- Boolean-based Blind SQL Injection: Exploits Boolean conditions to infer information about the database by observing changes in the application's response.
- Time-based Blind SQL Injection: Delays the server's response to SQL queries to infer information about the database structure or contents.

Second-Order SQL Injection:

- Injects malicious payloads into the application's data store, such as a database, for later execution under certain conditions. The injection occurs indirectly through user input that is stored in the database and later used in SQL queries.

Inferential SQL Injection:

- Similar to blind SQL injection, inferential SQL injection exploits the behavior of the application's responses to infer information about the database. Attackers use techniques such as time delays or content-based responses to extract data indirectly.

Deep SQL Injection:

- Targets vulnerabilities beyond the application layer, such as SQL injection vulnerabilities in stored procedures, triggers, or other database objects.

NoSQL Injection:

- Exploits vulnerabilities in NoSQL databases by injecting malicious queries or payloads into non-relational database systems that use query languages like MongoDB's Query Language (MQL).

Each mode of SQL injection attack targets different weaknesses in web applications or database systems, emphasizing the importance of comprehensive security measures, including input validation, parameterized queries, and regular security assessments, to prevent exploitation.

SQLIA Detection Approaches

Static Approach:

Software engineers give a few rules for SQLIA detection amid web application advancement, and this methodology is otherwise called the pre-creating approach. For the pre-created technique for identifying SQLIA as having compelling legitimacy checking component is required for the info variable information.

Dynamic Approach:

Post-created methods are helpful for the examination of elements. or SQL query on runtime, produced by client information a web application, and consequently, this methodology is otherwise called the post-created approach. Detection methods works under this post-produced class, executing before presenting a query on the database server.

Detecting SQL injection vulnerabilities requires a combination of manual testing and automated scanning techniques. Some approaches are given below:

Manual Testing:

- **Input Validation Testing: Review the application's codebase to ensure that all user inputs are properly validated and sanitized before being used in SQL queries. Look for instances where user input is directly concatenated into SQL queries without proper validation.**
- **Error-Based Testing: Manipulate input fields to provoke error messages that may reveal underlying SQL syntax or database structure. For example, entering single quotes or special characters into input fields may trigger SQL error messages.**
- **Union-Based Testing: Inject SQL UNION statements into input fields to combine the results of two SQL queries and retrieve additional information from the database. Monitor application responses for any unexpected data returned in the application's output.**
- **Blind SQL Injection Testing: Use Boolean-based or time-based techniques to infer the existence of SQL injection vulnerabilities without direct access to error messages or query results. Modify input parameters and observe changes in the application's response times or behavior.**

Security Headers and Logging:

- Implement security headers such as Content Security Policy (CSP) and X-XSS-Protection to mitigate the risk of injection attacks and provide additional protection against cross-site scripting (XSS) vulnerabilities.
- Enable detailed logging of SQL queries and database interactions to track and analyze potentially malicious activity. Monitor logs for suspicious or unexpected queries that may indicate SQL injection attempts.

Static Code Analysis:

- Perform static code analysis using tools like SonarQube or Checkmarx to identify potential security vulnerabilities, including SQL injection, in the application's source code. These tools can automatically scan codebases for insecure coding practices and provide recommendations for remediation.

Regularly testing and monitoring web applications for SQL injection vulnerabilities is essential to identify and address security weaknesses before they can be exploited by attackers. Additionally, incorporating security into the software development lifecycle (SDLC) through secure coding practices and continuous security testing can help prevent SQL injection vulnerabilities from being introduced in the first place.

Prevent SQLIA

Preventing SQL Injection attacks involves a combination of best practices in coding, input validation, and utilizing security features provided by database management systems. Some key measures to prevent SQL Injection attacks are given below:

Use Parameterized Queries or Prepared Statements: Instead of concatenating user input directly into SQL queries, use parameterized queries (also known as prepared statements) provided by your programming language's database API. This separates the SQL code from the data, preventing injection attacks.

Input Validation and Sanitization: Validate and sanitize all user input before using it in SQL queries. This involves checking input against an expected format or whitelist of allowed characters and rejecting or sanitizing any input that does not meet these criteria.

Least Privilege Principle: Use the principle of least privilege when setting up database permissions. Ensure that database users have only the necessary permissions required for their tasks. Avoid giving unnecessary write or execute permissions to database users.

Escaping Special Characters: If you cannot use parameterized queries or prepared statements, escape special characters in user input before including them in SQL queries. Different database management systems provide functions for escaping characters.

Use ORM (Object-Relational Mapping) Libraries: ORM libraries abstract database interactions and often provide built-in protections against SQL injection attacks. However, it's essential to use these libraries correctly and understand how they handle database queries behind the scenes.

Avoid Dynamic SQL: Minimize the use of dynamic SQL, where SQL queries are constructed dynamically based on user input. If dynamic SQL is unavoidable, ensure that proper validation, parameterization, and escaping techniques are applied.

Update and Patch Software: Keep your database management system, web server, and application frameworks up-to-date with the latest security patches. Vulnerabilities in these components can be exploited by attackers.

Implement WAF (Web Application Firewall): Use a WAF to filter and monitor HTTP traffic to and from a web application. Modern WAFs often include SQL injection detection and prevention capabilities.

Regular Security Audits and Penetration Testing: Conduct regular security audits and penetration testing to identify and address any vulnerabilities in your application's codebase and infrastructure.

Educate Developers: Train developers on secure coding practices, including awareness of common vulnerabilities like SQL injection. Encourage code reviews and peer feedback to ensure compliance with security best practices.

By following these practices, one can significantly reduce the risk of SQL Injection attacks in web applications.

Conclusive Discussion

This article has demonstrated the mode, detection, and prevention of SQL injection attacks. SQL injection attacks remain one of the most prevalent and damaging security threats to web applications and databases. They exploit vulnerabilities in input validation and SQL query construction, allowing attackers to execute arbitrary SQL commands and gain unauthorized access to sensitive data, manipulate database contents, or even compromise the entire system.

References

[1] William G. J. Halfond, Jeremy Viegas, and Alessandro Orso, (2006) "A Classification of SQL Injection Attacks and Countermeasures", 2006 IEEE

[2] Ankita Kushwah, Gajendra Singh (2014) "SQL Injection Attacks: Prevention for All Types of Attacks", International Journal of Emerging Engineering Research and Technology Volume 2, Issue 2, May 2014, PP 37-42

[3] Gregory T. Buehrer, Bruce W. Weide, and Paolo A. G. Sivilotti (2005) "Using Parse Tree Validation to Prevent SQL Injection Attacks" , 2005 ACM 1595932044/05/09

[4] Neha Mishra, Sunita Gond (2013) "Defences to Protect Against SQL Injection Attacks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013

[5] Parveen Sadotra (2015) "Hashing Technique - SQL Injection Attack Detection & Prevention", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 5, May 2015

[6] Dr. Manju Kaushik, Gazal Ojha (2014) "SQL Injection Attack Detection and Prevention Methods: A Critical Review", International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 4, April 2014

[7] Sayyed Mohammad Sadegh Sajjadi and Bahare Tajalli Pour (2013) "Study of SQL Injection Attacks and Countermeasures", International Journal of Computer and Communication Engineering, Vol. 2, No. 5, September 2013

Dr R. P. Mahapatra and Mrs Subi Khan (2012) "A Survey of SQL Injection Countermeasures", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.3, June 2012

[9] Sammangi Gowtam Pratap Kumar, Akula Sai Chanukya, Ayinavalli Venkata Ramana (2014) "Collaborative Technique to Detect and Prevent SQL Injection Attacks", International Journal of Advanced Computer Communications and Control Vol. 02, No. 02, April 2014

[10] Sruthi Bandhakavi, Prithvi Bisht, P. Madhusudan, V. N. Venkatakrishnan (2007) "CANDID: Preventing SQL Injection Attacks using Dynamic Candidate Evaluations", 2007 ACM 978-1-59593-703-2/07/0011

[11] Pooja Saini, Sarita (2015) "Survey and Comparative Analysis of SQL Injection Attacks, Detection and Prevention Techniques for Web Applications Security", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169, Volume: 3 Issue: 64148 – 4153

[12] Chris Anley (2002) "Advanced SQL Injection in SQL Server Applications", An NGS Software Insight Security Research (NISR) Publication ©2002 Next Generation Security Software Ltd http://www.ngssoftware.com

[13] Tejinderdeep Singh Kalsi, Navjot Kaur (2015) "Detection and Prevention of SQL Injection Attacks Using Novel Method In Web Applications", Kaur et al., International Journal of Advanced Engineering Technology E-ISSN 0976-3945

[14] Sonam Panda, Ramani (2013) "Protection of Web Application against SQL Injection Attacks", International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol.3, Issue.1, Jan-Feb. 2013 pp-166-168 ISSN: 2249-6645

[15] J. Makesh, S. Thirunavukarasu (2015) "SQL Injection Attack", Special Issue of Engineering and Scientific International Journal (ESIJ) ISSN 2394-187(Online) Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College ISSN 2394-7179 (Print) (TSRW-MCA-SAEC) – May 2015.

[16] Mihir Gandhi, Jwalant Baria (2013) "SQL INJECTION Attacks in Web Application", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013

[17] Nanhay Singh, Khushal Singh, Ram Shringar Raw (2012) "Analysis of Detection and Prevention of Various SQL Injection Attacks on Web Applications", International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 2– No.7, May 2012 – www.ijais.org

[18] Nikita Patel, Fahim Mohammed, Santosh Soni (2011) "SQL Injection Attacks: Techniques and Protection Mechanisms", International Journal on Computer Science and Engineering (IJCSE) ISSN: 0975-3397 Vol. 3 No. 1 Jan 2011 199-203

[19] Atefeh Tajpour, Suhaimi Ibrahim, Mohammad Sharifi (2012) "Web Application Security by SQL Injection Detection Tools", International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012 ISSN (Online): 1694-0814 www.IJCSI.org 332

[20] Shubham Srivastava, Rajeev Ranjan Kumar Tripathi (2012) "Attacks Due to SQL Injection & Their Prevention Method for Web-Application", International Journal of Computer Science and Information Technologies, Vol. 3 (2), 2012, 3615-3618

[21] Kamlesh Kumar Raghuvanshi, Deen Bandhu Dixit (2014) "Prevention and Detection Techniques for SQL Injection Attacks", International Journal of Computer Trends and Technology (IJCTT) – volume 12 number 3 – Jun 2014

[22] Manisha A. Bhagat, Prof. Vanita Mane (2013) "Protection of Web Application against Sql Injection Attack", International Journal of Scientific and Research Publications, Volume 3, Issue 10, October 2013 ISSN 2250-3153

[23] Bharti Nagpal, Naresh Chauhan, Nanhay Singh (2014) "Protection of Web Application Against SQL Injection Attack", Injection And Prevention off SQL Injection Attacks On Web Applications", IJSWS 14-393; © 2014

[24] Khaled Elshazly, Yasser Fouad, Mohamed Saleh, Adel Sewisy (2014) "A Survey of SQL Injection Attack Detection and Prevention", Journal of Computer and Communications, 2014, 2, 1-9, Published Online June 2014 in SciRes. http: // www.scirp.org / journal / jcchttp: // dx.doi.org /10.4236/jcc.2014.28001

[25] Ying Jin, Xiaoying Shen, Chunhui Song "A Filter-Based Approach for Sql Injection Attack Detection", https: // www.ecs.csus.edu / csc / iac / docs / publications/JIN_CATA12.pdf

[26] Etienne Janot, Pavol Zavarsky "Preventing SQL Injections in Online Applications: Study, Recommendations and Java Solution Prototype Based on the SQL DOM", https: // www.owasp.org / images / 5 / 57 / OWASP - AppSecEU08-Janot.pdf

[27] Zhendong Su, Gary Wassermann (2006) "The Essence of Command Injection Attacks in Web Applications", POPL '06 January 11.13, 2006, Charleston, South Carolina, USA. Copyright 2006 ACM 1-59593-02702/06/0001

[28] Asha. N, M. Varun Kumar, Vaidhyanathan. G (2012) "Preventing SQL Injection Attacks", International Journal of Engineering Applied Sciences and Technology, 2016 Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 23-29

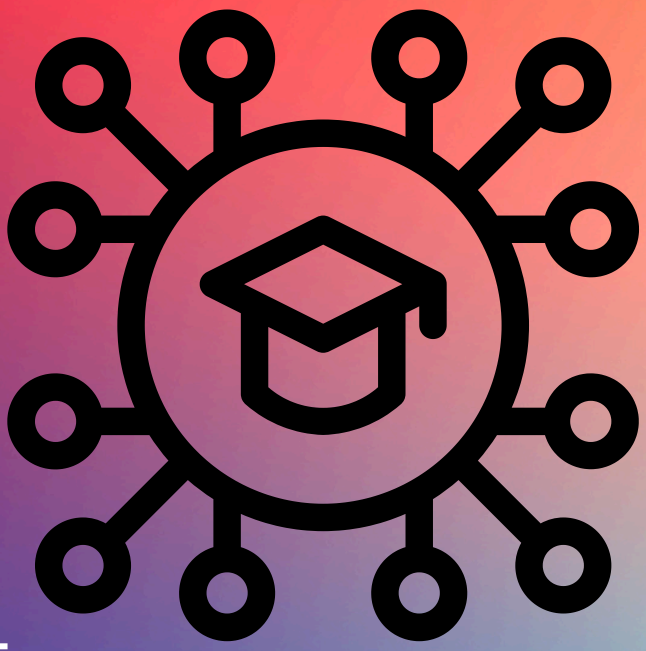
[29] Ms. Mira K. Sadar, Mr. Pritish A. Tijare, Mr. Swapnil N. Sawalkar (2014) "Securing Web Application against SQL Injection Attack: A Review", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 2 Issue: 3 683 – 687

[30] Neha Singh, Ravindra Kumar Purwar (2012) "SQL INJECTIONS – A HAZARD TO WEB APPLICATIONS", International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 6, June 2012 ISSN: 2277 128X

{31] Shelly Rohilla, Pradeep Kumar Mittal (2013) "Database Security by Preventing SQL Injection Attacks in Stored Procedures", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013 ISSN: 2277 128X

[32] Derrick Hyatt (2009) "Web 2.0 Injection Infection Vulnerability Class", ISSN: 1939-3555 (Print) 1939-3547 (Online) Journal homepage: http://tandfoline.com /loi/uiss20

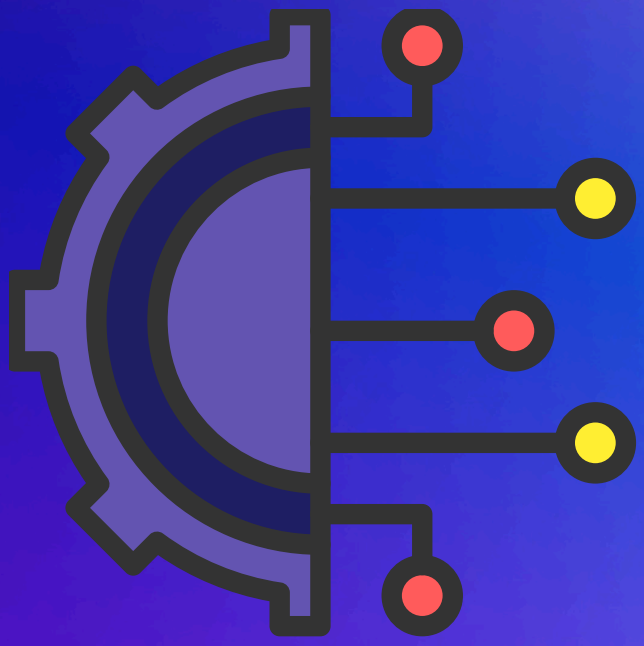
[33] https://portswigger.net/web-security/sql-injection (Last accessed on 1st May 2024)



Let us peep into the Deep of Learning

By- Dr Munmun Biswas

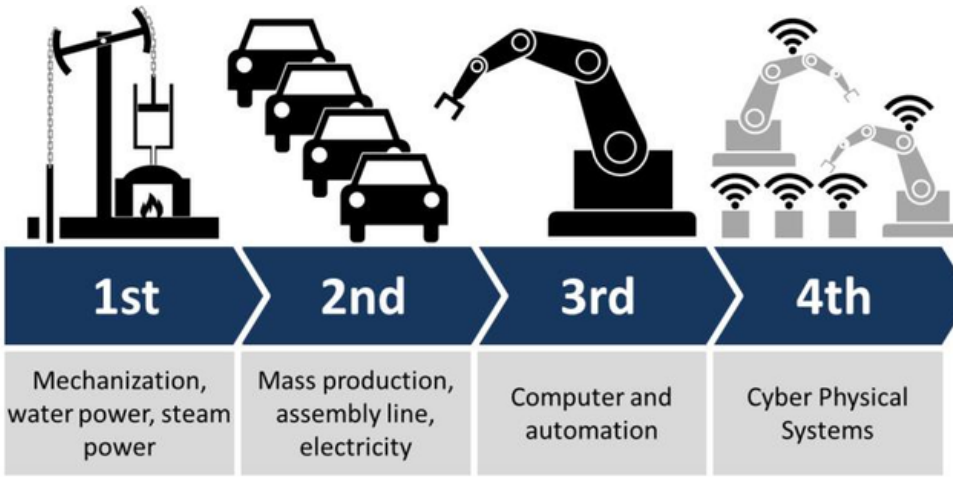
Assistant Professor and HoD
Brahmananda Keshab Chandra College



As you may know, the subject area of Deep Learning (DL) is a special part of the subject area of Machine Learning (ML). Now these ML algorithms provide you the main toolbox for all artificially intelligent devices to work. In this article we will try to get a very brief introduction to the topic.

What learning is meant over here?

Clearly, we want our computer to learn. The most precious machine of the day, which can automate all other man-made machines is our computer. It was called the third industrial revolution when the age of computers started. And now? We are in the age of the fourth industrial revolution. We all are talking about the AIs, the IoTs, Big Data analytics, crypto currency and all that. This means we already have upgraded our computers to an immensely higher computational speed and efficiency. The CPUs have been replaced by GPUs (Graphics Processing Units). Hence we can see the computers' ability has been raised to imitate human ability to a greater extent.

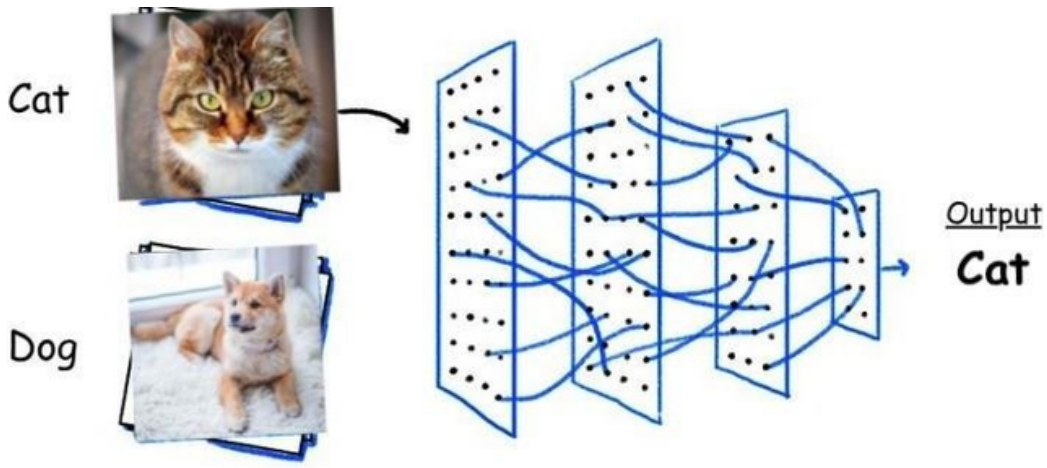


How computers could play chess?

In the early days of research on AI, people tried to make computer solve those problems which were difficult for human brain to tackle in small time. IBM's chess playing program, named Deep Blue defeated the world chess champion Garry Kasparov in 1997. How computer can play chess? The idea is to check for all possible moves and its consequences at each stage of the game. This is nothing but how one human player fixes his or her move. Definitely a properly programmed computer can systematically check for larger number of possibilities than a human player in real time.

What was the challenge next?

The next challenge for AI researchers was on- how computers could perform those tasks which are almost immediate for human brain to perform but difficult to explain. Like, take the example of distinguishing a dog from a cat, say, both of equal sizes. A human baby learns to distinguish a dog from a cat by experience. How then computer can learn to differentiate pictures of a dog from the pictures of a cat, from a number of pictures of either a dog or a cat? This is the well known problem of classification, falls under the category of supervised learning.

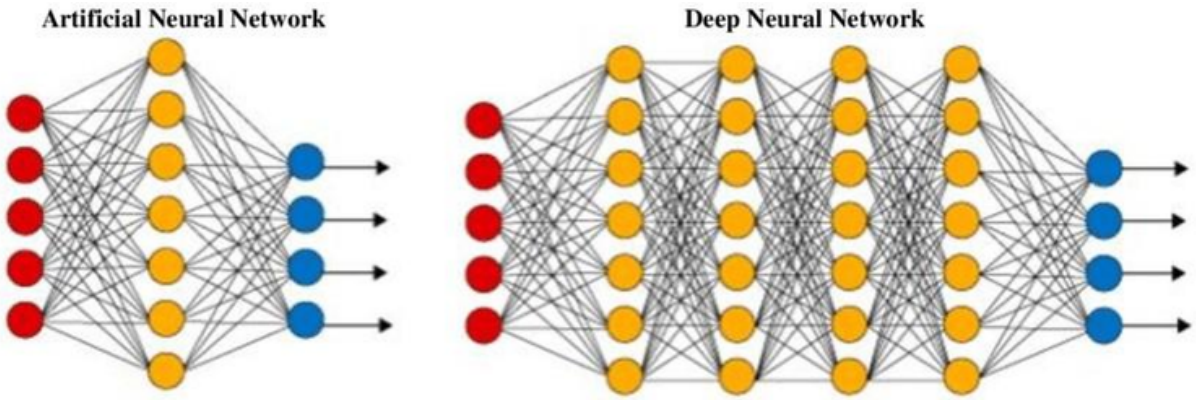


Neural Networks

Neural network is the most important kind of computational model (or algorithm) which consists of interconnected nodes (or neurons) that process or learn from data (or information/ experience). As the name suggests it has been influenced by the way human brain works or learns from experience. Human brain primarily collects leveled information through neurons. These neurons are inter-connected to exchange electric signals within themselves.

The leveled information is the training data for the human brain. This helps the brain to take future decisions or to make future leveling.

The single layered perceptron is the simplest artificial neural network (ANN) architecture. It was introduced by Frank Rosenblatt, a respected psychologist. But perceptron showed some limitations in handling non-linear functions. In 1986 a few researchers shed lights on hidden layers of neurons. In 2006, finally researchers discovered multi-layered neural network model suitable for Deep Learning, called Deep Neural Network (DNN).



In the above image (taken from the internet) reds are the input nodes, yellows are the nodes from the hidden layers, blues are the output nodes.

Applications

Without going into much technical details of neural network let us illustrate how the above mentioned classification problem (distinguishing pictures of dogs and cats) can be solved by using neural network. We can feed computer with a training data set of thousands of images of cats and dogs mentioning their levels. Let us level a picture of dog to be 0 and that of a cat to be 1.

On the basis of that training data a neural network model can be built a classification model. Then on the basis of this model now for a test data (a new picture here, of either a dog or a cat) the computer can predict the level, either 0 or 1. Before we end, a few applications of Neural network based programs can be mentioned. By using it one can differentiate within vehicle, animal, person for a driving camera. Neural network can be designed to distinguish between safe and fraudulent bank transactions. It is also being used in hand writing and speech recognition problems. All these are problems of Deep Learning along with many other problems, which students can search for their further interest.

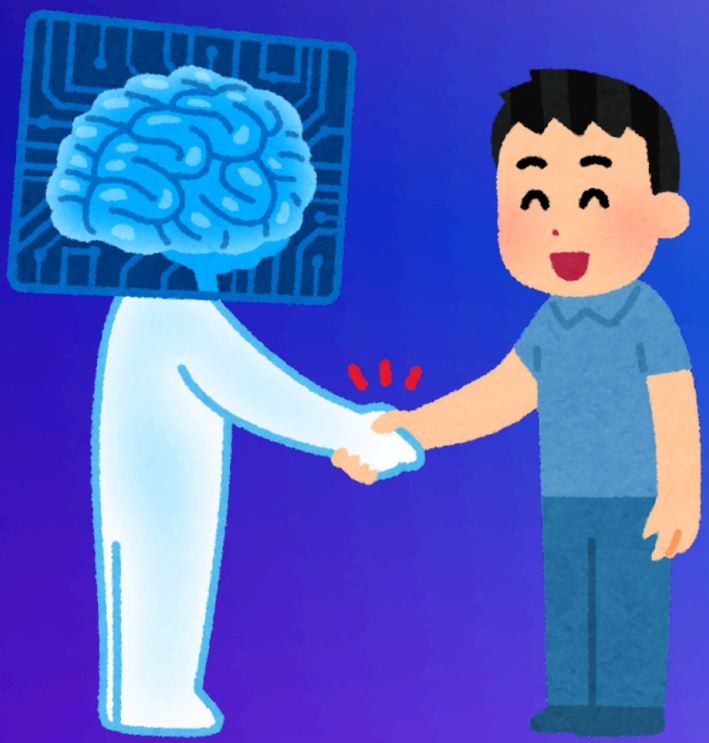
References

1) (https://www.freecodecamp.org/news/simple-chess-ai-step-by-step-1d55a9266977/)

Images Credits: Google

Deciphering the Black Box: Explainable AI Techniques in Healthcare

By- Dr. Tuhin Utsab Paul
Associate professor and HoD
St. Xavier's University, Kolkata



The delivery, diagnosis, and treatment of healthcare have all seen radical changes in recent years due to the explosive growth of Artificial Intelligence (AI) technology. Specifically, machine learning algorithms have proven to be exceptionally adept at sifting through enormous amounts of medical data, finding trends, and offering insightful information for clinical decision-making. AI-driven solutions have the potential to greatly improve patient outcomes, lower medical mistakes, and increase the overall effectiveness of health-care systems in a variety of contexts, from illness diagnosis and risk estimation to treatment optimization and patient monitoring.

But as healthcare organizations depend more and more on AI algorithms to help with crucial decision-making procedures, worries about these algorithms' opaque nature have grown. Deep neural networks and other conventional machine learning models frequently function as opaque systems, making it difficult to comprehend the reasoning behind their judgements or predictions. A major barrier to the mainstream acceptance and deployment of AI technology in healthcare settings is its lack of explainability, as transparency, understanding, and trust are critical elements.

The field of explainable artificial intelligence (XAI) has gained significant traction as a means of tackling the problems of interpretability and transparency that come with complicated AI systems, especially those used in healthcare. XAI approaches aim to close the gap between the predictive capability of AI models and the requirement for human comprehensibility and responsibility in decision-making processes by improving our knowledge of how AI algorithms make judgements.

One cannot stress the significance of explainability in the medical field. Stakeholders such as patients, regulatory agencies, clinicians, and others need to trust the judgements made by AI systems and comprehend the underlying reasons that shape those decisions. Moreover, explainability is essential to guaranteeing that AI-powered medical interventions respect patient choices, clinical best practices, and ethical standards.

An interdisciplinary approach that incorporates ideas from a wide range of disciplines, including as computer science, statistics, cognitive psychology, and human-computer interaction, is fundamental to the fundamental ideas of XAI. Scholars working in the field of XAI attempt to achieve a fine balance between interpretability and model complexity in order to guarantee that the explanations given are correct and understandable to end users. Leading the pack in these approaches are post-hoc explanation techniques like SHAP and LIME, which are well-known for their ability to provide both local and global explanations for black-box models, providing information on the role that various features play in model predictions. Furthermore, interpretability approaches particular to models, such as Layer-wise Relevance Propagation (LRP) and GradCAM, offer visualizations that draw attention to the important areas of the input data that influence the decisions made by the model.

Furthermore, XAI's foundations go beyond technical approaches to include deep ethical questions and societal ramifications. There is a growing need to guarantee justice, openness, and accountability in AI decision-making processes as these technologies are incorporated into daily life. To solve issues with prejudice, discrimination, and privacy in AI systems, ethical frameworks, rules, and legislation are being created. Fundamentally, the XAI framework emphasizes how critical it is to apply a human-centric design approach, in which AI systems are created with close attention to the requirements, values, and preferences of users.

One cannot stress the significance of explainability in the medical field. Stakeholders such as patients, regulatory agencies, clinicians, and others need to trust the judgements made by AI systems and comprehend the underlying reasons that shape those decisions. Moreover, explainability is essential to guaranteeing that AI-powered medical interventions respect patient choices, clinical best practices, and ethical standards.

An interdisciplinary approach that incorporates ideas from a wide range of disciplines, including as computer science, statistics, cognitive psychology, and human-computer interaction, is fundamental to the fundamental ideas of XAI. Scholars working in the field of XAI attempt to achieve a fine balance between interpretability and model complexity in order to guarantee that the explanations given are correct and understandable to end users. Leading the pack in these approaches are post-hoc explanation techniques like SHAP and LIME, which are well-known for their ability to provide both local and global explanations for black-box models, providing information on the role that various features play in model predictions. Furthermore, interpretability approaches particular to models, such as Layer-wise Relevance Propagation (LRP) and GradCAM, offer visualizations that draw attention to the important areas of the input data that influence the decisions made by the model.

Furthermore, XAI's foundations go beyond technical approaches to include deep ethical questions and societal ramifications. There is a growing need to guarantee justice, openness, and accountability in AI decision-making processes as these technologies are incorporated into daily life. To solve issues with prejudice, discrimination, and privacy in AI systems, ethical frameworks, rules, and legislation are being created. Fundamentally, the XAI framework emphasizes how critical it is to apply a human-centric design approach, in which AI systems are created with close attention to the requirements, values, and preferences of users.

XAI encourages greater patient engagement in their own healthcare journey by giving them insights into the reasoning behind AI-driven suggestions. The significance of XAI is further highlighted by ethical considerations, since transparent and interpretable AI systems are necessary to guarantee justice, responsibility, and reliability in healthcare applications. To fully utilize AI while maintaining patient safety, fairness, and ethical integrity, it is imperative that XAI be included into healthcare research and practice.

Explainable AI supports:

1. Patient Empowerment:

Patients are taking a more active role in their healthcare journey and are interested in knowing the reasoning behind suggestions made by AI systems, which is influencing clinical decision-making processes. In this sense, interpretable explanations of AI predictions and conclusions provided by XAI are crucial in empowering patients to make well-informed decisions regarding their treatment regimens.

Patients may take an active role in shared decision-making with their healthcare professionals thanks to XAI, which demystifies AI algorithms and promotes transparency in decision-making. This empowerment improves treatment adherence and health outcomes in addition to increasing patient autonomy and involvement. Furthermore, XAI encourages a collaborative approach to healthcare delivery where patients are seen as stakeholders in the decision-making process rather than as passive beneficiaries of care by fostering patient centered care.

2.Clinician Understanding:

These technologies are being used by physicians more and more to help with patient care, diagnosis, and treatment planning. XAI helps doctors make more educated clinical decisions by providing a clear explanation of the reasoning behind AI driven suggestions. This allows clinicians to assess and trust these recommendations critically. Additionally, XAI promotes accountability and openness in AI systems, enabling medical professionals to recognize and correct any bias. However, the application of XAI in healthcare raises clinician's confidence while simultaneously improving the caliber and effectiveness of clinical decision-making.

3.Bias Mitigation:

The possibility that AI-driven systems could unintentionally reinforce biases found in the training data is becoming more widely recognized. By giving interpretable reasons for AI predictions, XAI techniques provide a way to detect and reduce bias and allow stakeholders to examine model decisions and pinpoint areas of concern. XAI helps to identify and fix biased trends in AI algorithms by illuminating the variables affecting model predictions.

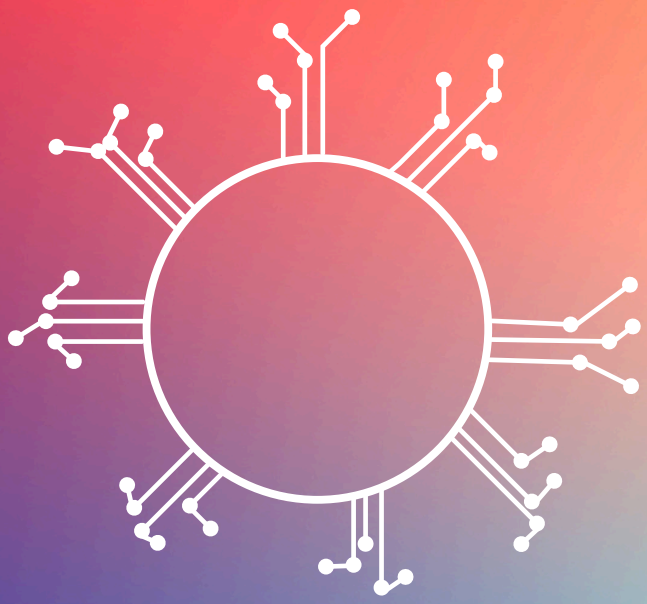
Furthermore, XAI fosters accountability and transparency in healthcare AI applications by enabling academics and clinicians to evaluate the justice and equity of AI systems. The incorporation of XAI into healthcare strengthens attempts to reduce bias, which in turn improves the integrity, fairness, and equity of AI-driven decision-making processes.

4. Regulatory Compliance:

The increasing adoption of AI technologies for many clinical applications necessitates adherence to regulatory norms, including the Health Insurance Portability and Accountability Act (HIPAA). In this sense, XAI techniques are essential because they offer comprehensible justifications for AI judgments and forecasts, allowing interested parties to comprehend and examine the parameters influencing model results. Enhancing accountability and transparency in AI-driven systems, XAI makes it easier to comply with laws pertaining to data security, privacy, and the moral application of AI in healthcare.

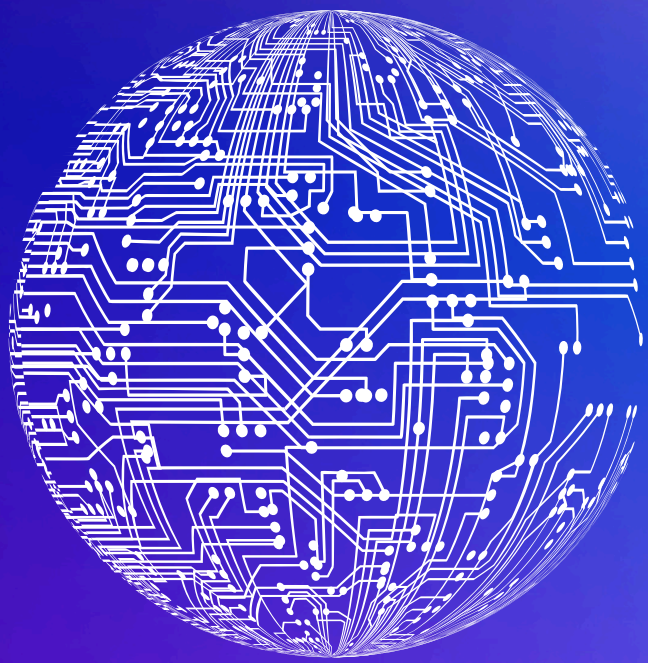
XAI also facilitates the creation of standards and guidelines for the appropriate application of AI systems in clinical practice by giving regulatory bodies and healthcare organizations the capacity to evaluate the safety, fairness, and dependability of these systems.

Generally, the demands of the healthcare application such as the kind of data, the model architecture, and the criteria for interpretability determine which XAI approach is best. To provide relevant insights and actionable interpretations for clinical decision- making and patient care, researchers and practitioners must carefully assess the strengths and limits of each technique in their unique contexts. To overcome obstacles and promote the use of interpretable AI in healthcare, more study and development are required.



Understanding the Data Structures and Algorithms in an easy way.

By- Mr Partha Sarathi Gupta
Assistant Teacher
Dighalgram Netaji Vidyapith High School



Introduction:

Data Structures and Algorithms is that topic of Computer Science without which knowledge on Computer Science subject is incomplete. Without a solid understanding of data structures and algorithms we may struggle to write efficient code, leading to develop slower or less scalable software. They are fundamental to problem-solving in computer science. Without this knowledge, we may find it difficult to tackle complex programming challenges. We use this topic in day to day to life knowingly or unknowingly in our daily life too. Data can be arranged in many ways but mathematical and logical arrangements of data are known as Data Structures and Algorithms are consecutive steps for solving problems and to perform computations. Actually we can say that while solving a problem we need to store the data efficiently by using data structures, so that we can fetch and do operations on those data quickly and efficiently whereas by use of algorithms we also develop logics to solve the problems very efficiently. So we can conclude that we need both to solve a particular problem. Let's know it more.

Classifications:

Data Structures are classified in two categories as:

1) Linear: In this type of data structure data elements are arranged sequentially or linearly, here each element is attached to its previous and next adjacent elements. This is further classified in two categories they are:

Static data structures: It has fixed memory size. Whose size cannot be altered during run time. Example: Static Array

Dynamic data structures: Here the size of memory is not fixed. It can be randomly updated during the runtime which may be considered efficient concerning the memory. Example: Linked List

2) Non Linear: In this type of data structure data elements are not arranged sequentially or linearly. We can't traverse all the elements in a single run only. Example: Trees and Graphs.

Operations on different Data Structures:

Traversing: It means to visit the element stored in it.

Searching: It means to find a particular element in the given data-structure.

Insertion: It means to add an element in the given data structure. Deletion: It means to delete an element in the given data structure. Sort : Sorting data in a particular order (ascending or descending).

Merge: Merging data of two different orders in a specific order may ascend or descend.

We can use algorithms in many use cases like for searching, sorting and to deals with graphs. Algorithms can be classified according to the problem solving strategies like:

1) Dynamic programming algorithms: They are implemented to solve problems by breaking them down into smaller sub problems.

2) Brute force algorithms. By trying all possible solutions until the correct one is found.

3) Recursive algorithms. These algorithms call themselves with smaller input values and use the results of these calls to solve the current problem.

4) Greedy Algorithms. Greedy algorithms make locally optimal choices at each step with the hope of finding the global optimum.

5) Divide and conquer algorithms. These algorithms divide the problem into smaller sub problems, solve them independently, and then combine their solutions to solve the original problem.

6) Backtracking algorithms. They work by trying different solutions and backtracking to find the correct solution when a dead end is reached.

7) Randomized algorithms. Randomized algorithms use random numbers to make decisions during the execution, which means they can give different outputs on different runs.

Let's know how to make an efficient algorithm:

Asymptotic Analysis- It is a type of mathematical analysis used to classify algorithms based on their running time or space requirements. It is an invaluable tool for developers, as it allows them to better understand and optimize the performance of their programs.

There are mainly three asymptotic notations:

1. Big-O Notation (O-notation)- Maximum time required for program execution.

2. Big-Omega Notation (Ω -notation)- Minimum time required for program execution.

3. Big-Theta Notation (Θ-notation)- Average time required for program execution.

Concepts on few important data structures:

Array:

An array is a data structure consisting of a collection of elements which are stored in contiguous memory location, each identified by an index or key. For example, let's consider we want to store some numbers. [1,5,7,0] This could be an array. We need a contiguous block of memory that could hold this array.

Linked List:

Arrays are useful, but they suffer from a pretty big disadvantage. As the array increases or decreases in size, we have to do all sorts of memory gymnastics. As we increase the size of the array, newer chunks of memory still need to be allocated.

Hash Table:

We are trying to store key value pairs. For instance, we have (person name, age) as a possible data structure we wish to store. Or maybe we want to store (identifier, person object) as a key value pair. So given an identifier, we want to quickly retrieve the person object.

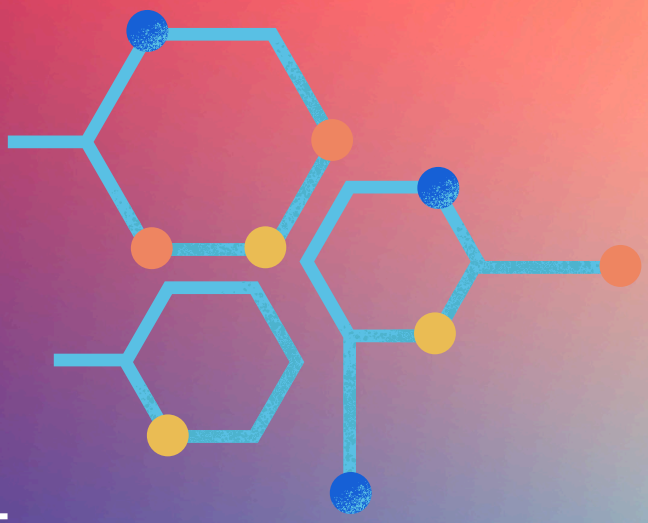
Well, that's where a hash table fits. Let's first define what a hash is. A hash is a function that we pass into an object and it reliably, for the same object, gives us the same hash every time. Given that, if we were to pick a hash function and pass in an identifier, it would yield us a number where we can store a pointer to the person object.

Tree

A tree is quite similar, except, in a linked list, we can link to only one other node. In a tree, we can link to multiple other nodes. A binary tree can link to exactly two other nodes. Also, a tree cannot be a loop. This means that element 1 cannot point to element 2 and then to 3, and 3 point back to 1. Tree can be of different types like: Binary Tree, Ternary Tree, Generic Tree. Some special types of trees are there like: Binary Search Tree (It is very useful to search an element in tree), AVL Tree (AVL tree is a self-balancing Binary Search Tree (BST) where the difference between heights of left and right subtrees for any node cannot be more than one or less than minus one.), B-Tree (It is also a self-balancing search tree.), B+Tree (B+ tree eliminates the drawback B-tree)

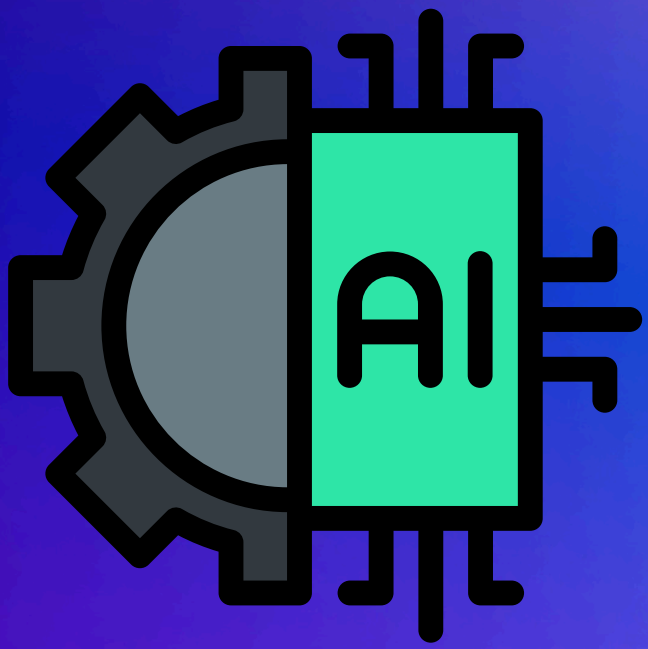
Conclusion:

Data structures and algorithm analysis are fundamental concepts in computer science that underpin the development of efficient software solutions. By leveraging appropriate data structures and analyzing algorithm efficiency, programmers can design robust, scalable, and optimized solutions to a wide range of computational problems. Understanding these concepts equips developers with the tools to tackle complex problems and build innovative software applications that power our digital world



Intersection of Data Science and AI

By-Simerjeet Singh Bedi
2nd year Student
Department of Computer Science
Dum Dum Motijheel College



Data Science is a field or Subject that Concerns with using Maths and Statistics along with tools like Artificial Intelligence and Machine Learning to analyze and Uncover patterns and Trends to solve Structured and Unstructured data Problems. And which can be used for

Creating predictive models as well.

Data Scientist are in huge demand everywhere in the world and the reason behind it is their data science skills.According to the report of linkedin U.S emerging jobs report 2020,

Data scientist is a field which is ranked #3 with 37% annual growth.

Now the question is why data science ?

The graph of growth of data is constantly increasing.

Now to fulfill this demand we need more and more data scientists who will analyze it with their statistical methods to convert it into organized data which is of good use.

Data science is also needed to create a better customer experience.

Data science along with the use of AI and machine learning create predictive models which help organizations and companies to make user experience better . For example, an ecommerce site like flipkart uses the purchase history to give suggestions.

Data Science can also be used to help organizations and business to increase profitability.

To do this business first analyze data and then turn them into sensible insights which can be used to provide products and services in a better manner and to make the operations of the business better to work .Let's take an example of the Healthcare industry. Through data Science they provide prediction about disease occurrence and help in making strategies about the treatment and Patient care.

Now let us talk about Intersection of Data Science and AI

When Data Science and AI combine together they can help to solve tough problems .

Now about the intersection of data science and AI we first need to understand what AI is. Artificial intelligence can be defined as the simulation of human intelligence in an appliance making them do the task which requires the intelligence of a human .AI can create systems that can understand the environment and convert them into beneficial insights .

In contrast, data science Does it work by extracting insights from data which can be structured and unstructured .Artificial Intelligence require data for their functioning therefore data is a crucial part to make their system run .The type of data like quantity and quality have a direct effect on the performance of AI system .Now let us study about the impact of artificial intelligence in data science . Artificial intelligence has a very important and significant impact on data science .By the use of AI technologies we can accelerate the potential of data science by the use of AI. Data scientists can reduce the time consumption and make deeper insights and precise predictions. Some major Examples of Integration of Data Science and Artificial intelligence are in Healthcare, Finance, Marketing and Manufacturing in all these both Data Science and AI has given better results.

References :

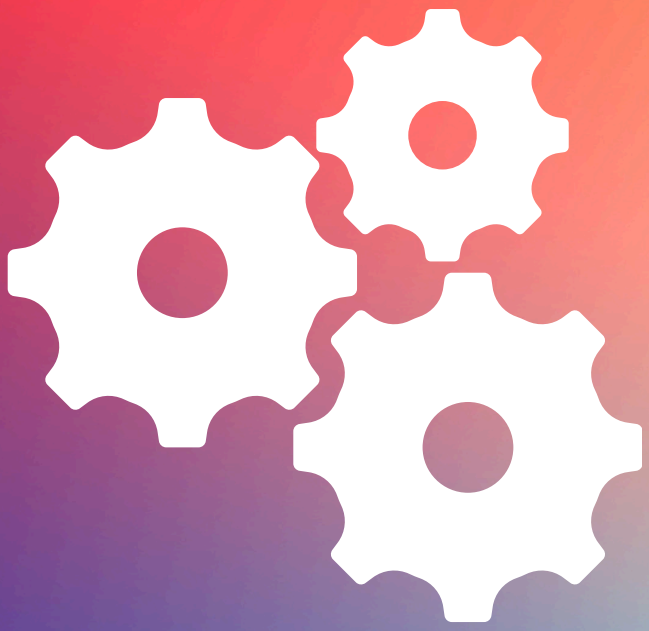
https://www.geeksforgeeks.org/why-do-we-need-data-science/

https://www.analytixlabs.co.in/blog/why-do-we-need-data-science/

https://www.datacamp.com/blog/what-is-data-analysis-expert-guide

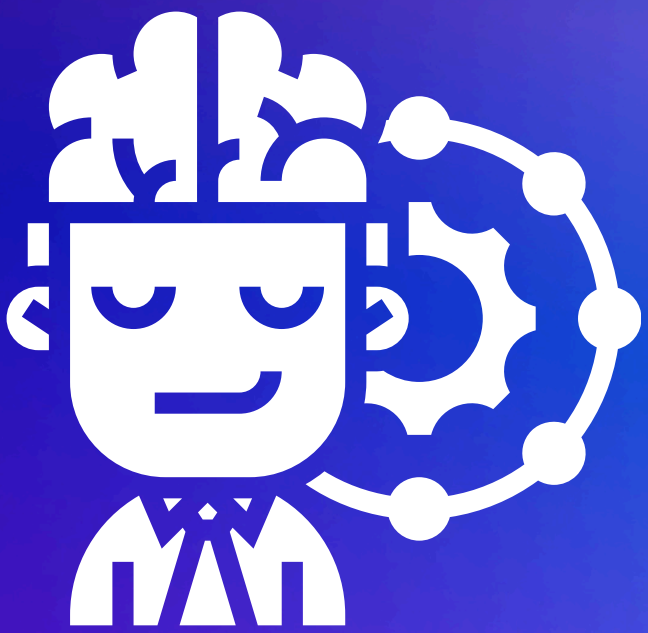
https://medium.com/@goproblogging/the-intersection-of-artificial-intelligence-and-data-science-3763830cf099

https://www.linkedin.com/pulse/how-use-data-ai-solve-real-world-problems-mariam-kili-bechir-/



Exploring the World of Machine Learning

By- Raja Das
2nd year Student
Department of Computer Science
Dum Dum Motijheel College



The core Idea of Machine Learning is – Teaching Machines to learn from data and step-by-step improving it without absolute programming.

Once which was a part of science fiction is now unknowingly a daily part of our life. The concept of machines which behave like human and has human like intelligence comes from *Samuel Butler's* 1872 novel *Erewhon*. Later the term '*Machine Learning*' was coined in 1959 by *Arthur Samuel*, an IBM employee and pioneer in the field of computer gaming and artificial intelligence. Now,

What is Machine Learning?

for those people who are unknown to the term, Machine Learning is a field of *Artificial Intelligence (AI)*, imagine a machine which can learn from experience, by identifying patterns, and can make decisions without definite programming. In a simpler way, it is like teaching a child to make difference in between objects and helping him/her to learn how to talk, walk etc. Just like that we provide these digital brains broad amount of data, images, numbers, text and step-by-step they improve and even can identify things which can be hard to identify in naked eyes.

The examples of Machine Learning can be very simple as –

1. **Facial or Pattern recognition –**

These days lack of personal data security is a major issue. Let us take a smartphone as example where we put a lot of personal information (E.g. Documents, pictures, contact info, etc). But if the smartphone gets to a wrong hand your personal data can leak and security can be at risk. To prevent it from happening every Smartphone company provide users with some level of security like Facial or Pattern recognition, where the device collects your finger print pattern or an image of your face to recognize the user of the device.

1. **Product recommendation –**

Do you ever wonder how major or minor product purchasing applications or several streaming applications can sometimes give you recommendation on what you might like to purchase and what you might like to watch. Simply the answer is with the help of machine learning. By analyzing the pattern of your search and the product you have purchased or the content you have seen, they provide you with a recommendation you might enjoy watching or item you might seem helpful to purchase.

1. **Voice to Text –**

Another simple use of Machine Learning you might have used but never knew is Voice to Text conversion. When you are busy or you have a lack of keyboard to write your search item or result you might have used the mic button present near the search bar, where you say in your mic and it detects the thing you are saying and searches the result.

And can be as broad as –

1. **Stock market forecasting and Fraud detection –**

Machine Learning is often actively being used in forecasting or predicting the future prices of Stocks and depending on the fluctuation trading decisions are made. And so, as Machine Learning slowly learn from patterns, it can help detect normal and abnormal behavior to spot suspicious activities, like money laundering and insider trading.

1. **Healthcare –**

Detecting medical conditions from MRIs, CT scans and X-rays, machine learning programs are often used to analyze the images and spot the abnormalities and other diseases. After detecting the disease with the help of data provided from the Machine Learning program, the patient can receive proper Healthcare.

(The uses of Machine Learning are many, only some examples are given here. To learn more examples or application of ML some resources are provided below)

Machine Learning is a developing topic and concerns regarding this topic are many –

1. **Bias and Fairness: Machine learning programs are trained using the data they are trained with. But if the data is biased the program will maintain that biasness and it may lead to unfair outcomes.**
2. **Privacy and Security: As described above Machine Learning programs are trained with large amount of data, and it raises concerns regarding leaking and misuse of personal data Privacy and Security.**
3. **Job Displacement: The daily and routine tasks once which were done by humans several of them are now being done by the Automative machines and developed Machine Learning to reduce errors. The sudden change raises concerns regarding job displacement or machines taking people's jobs**

(More problems or concerns regarding Machine Learning can be found in the internet and open sources. A resource is provided below for more details)

References :

https://hbr.org/2021/01/when-machine-learning-goes-off-the-rails

https://en.wikipedia.org/wiki/Samuel_Butler_(novelist)

https://en.wikipedia.org/wiki/Arthur_Samuel_(computer_scientist)

https://www.coursera.org/articles/machine-learning-in-finance

https://www.tableau.com/learn/articles/machine-learning-examples

Basic Fundaments of Cryptocurrency and Secure Navigation

By- Raja Das
2nd year Student
Department of Computer Science
Dum Dum Motijheel College

We people, who are used to public, private media, or social media services, have or often might have been introduced ourself with the term 'Cryptocurrency' with a form of an Add. Many people are used to the term Crypto or know what crypto is. But for the people who are unknown to the term,

"Cryptocurrency or in short Crypto is a form of Digital currency, which helps people to make transactions via online systems."

To give a brief history about crypto, it was first introduced as a form of digital coin called 'Bitcoin,' in January 2009, by a group of programmers - using the pseudonym Satoshi Nakamoto. The actual Identity of Nakamoto has never been verified. Some other examples of Crypto are – Ethereum, Tether, BNB, etc.

Now as we have been introduced ourself with Cryptocurrency and we know it is a form of Digital Currency, but a question arises,

What is the Difference between Regular Digital Currency and Cryptocurrency?

The regular Digital Currency we use or CBDC (Central Bank Digital Currency) is controlled by the Central Bank. It operates like the physical currency we use in our daily life. The central bank is responsible for the management of the money.

On the other hand, Cryptocurrency is an independent Digital currency which is not being controlled or backed by any Government and Banks. By using encryption method, it operates secure transaction and creation of more digital currency.

What is Blockchain technology?

Blockchain technology is a distributed ledger that is secure, transparent, and immutable. In Blockchain technology there are Blocks on which information is stored for secure transactions.

As we learned from above Cryptocurrency is used in buying or selling goods, but like regular investments another question might come to your brain,

Is Crypto or Cryptocurrency safe?

If you are interested in investing in cryptocurrencies, you need to know that, cryptocurrencies are usually built using Blockchain. The transactions are saved in 'Blocks' and with this it is possible to make safe transactions without any 3rd-party tampers.

To make the process more secure two-factor authentications are applied. Like when you put your password and user-id, you might receive a message for an OTP (One Time Password) for further conformations.

But,

'Where wealth accumulates, so does the potential for crime.'

Fraud and Scams

Fake websites are now nearly daily occurrence for online thieves to steal your money. These fake websites feature massive returns in case you invest money on their currency.

Scammers promote their fake currency on their websites by saying, that they have invested in their currency and whoever invests in it will receive large returns. Once enough people invest in it and the price of the product increases, those scammers cash out their investments and the total price of the currency drops by investors receiving massive losses.

These days deepfake of things are getting so real that it is hard to recognize between real and fake in naked eyes. Scammers using deepfake makes video of celebrities or Billionaires, promoting a specific cryptocurrency and asking investors to invest in that currency, and following the same steps given the paragraph above they scam a lot of people of their hard-earned money.

(There are more scams being held by online or offline thieves, to scam normal people of their money, only a few examples are given above. To know more about them and be aware about them please read or follow online media services and news channels.)

INow, how do you invest Safely?

As investing in crypto can be in your to-do list, you must follow the proper steps to invest in crypto Safely. Here are some small steps –

Do your research: Before investing in crypto, take the time to understand what cryptocurrency is, how it works, and the risks involved in it. There are many online resources, courses, and books available to help you learn.

Secure your investments: once you accumulate enough cryptocurrency you must take measure to keep it secure. Like keeping them in a pen-drive and enabling more security measures like two-factor-authentication.

Stay informed: Once you start investing you must keep yourself updated on your invested products and make your decisions with proper measures.

Stay patient: Cryptocurrency markets can be highly unstable, and prices can fluctuate wildly in the short term. Be patient and avoid making impulsive decisions based on short-term price movements.

References:

https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency)

Uncovering Insights related to Dark Web

By- Ananta Pandit
2nd year Student
Department of Computer Science
Dum Dum Motijheel College

The dark web officially appeared in the early 2000s with the creation of the Free Net. It was developed by Ian Clarke to secure users against government intervention and cyber-attacks. The system permits users to express themselves freely without being tracked online. The U.S. Naval Research Laboratory funded The Onion Router (TOR). TOR offered intelligence sources a way to communicate easily and safely, especially in hostile areas where personal key is safety. Nowadays, it's one of the most common browsers used to access the dark web.

What is the dark web?

The dark web encodes online content and gets permission from individuals to conceal their identity and location from others. It's content that's not listed by regular search engines. It is also known as the dark net. The dark web constitutes a large part of illegal activity on the internet. To a lesser extent, it is also used for lawful reasons by legal users, such as those who want to protect the privacy of certain information. To access the dark web, users must install a private browser like the The Onion Router(TOR) browser, use a Virtual Private Network(VPN) and ensure their computers are safe and secure.

What is the difference between the dark web and the deep web?

The deep web refers to parts of the internet not fully accessible through standard search engines like Google, Chrome, Yahoo!, etc. The deep web includes pages that were not listed, fee-for-service (FFS) sites, private databases, and sites found on the dark web. Hence, sometimes the term deep web is mistakenly used to refer to a dark web. Deep web pages can be accessed by anyone with a standard web browser who knows the Uniform Resource Locator (URL). Whereas dark web pages need special software and knowledge of where to find the content.

How does the dark web work?

Almost all people consider the dark web to be a place where online marketplaces for drugs, weapons deals, money laundering, exchanges for stolen data, and other illegal activities occur. There are many legal reasons people choose to use the dark web, including political dissidents and those who want to keep certain information private.

Regular search engine links allow Google and other search engines to return relevant results whenever a user types a keyword into the search bar. Websites on the dark web are not listed by regular search engines. As an alternative, the dark web uses information from individual email or social media accounts, databases, and documents to give users access.

How is the dark web accessed?

The dark web can't be accessed through regular browsers such as Firefox, Chrome, Google, Yahoo!, etc. It can only be accessed through an encoded peer-to-peer network connection or by using an overlay network, such as the TOR browser. The TOR browser is free to download and use and works with all major operating systems. It's short for The Onion Router, which ensures complete anonymity on the dark web by using multiple layers, a network of relays, and a traffic-routing mechanism that randomly bounces internet traffic through these relays, rendering an IP address untraceable. At the start, the TOR browser was developed and entirely used by the U.S. Navy to protect sensitive government communications.

Is it illegal to access the dark web?

It isn't illegal to access the dark web. It provides individuals with privacy and anonymity that regular websites don't offer. In spite of this, people can go on the dark web and post their thoughts about political activity without being insulted by government officials and other groups.

Is the dark web dangerous?

The dark web is a hotbed of criminal and illegal activity for buying and selling illegal drugs, weapons deals, and money laundering. Dangerous sites for browsing the dark web include the following:

- **Phishing**
- **Identity theft**
- **Credential theft**
- **Spying**
- **Leaks of intellectual property or trade secrets**

These dangers can interrupt business operations, cheat a company, and undervalue a brand's honesty. The greatest way to avoid these dangers is to avoid using the dark web completely. But if this is unworkable, it's important to employ reliable security measures, including antivirus software, and to access dark web sites only via a Virtual Private Network (VPN). For additional protection, there should be regular monitoring of the dark web to identify indicators of dark web compromise, such as database dumps or the posting of personal or financial information.

What are the disadvantages of using the dark web?

The dark web is used to remain anonymous when using the internet. It is easy to infect your machine while searching the dark web. It is unregulated, providing less protection to users. As a result, it is easy to infect your machine by clicking links or downloading information. You could also be exposed to malware, viruses, and other harmful content, scammed or phished, or have your personal information stolen.

References:

- https://www.techtarget.com/whatis/definition/dark-web
- https://www.investopedia.com/terms/d/dark-web.asp


Shot on OnePlus
Powered by Triple Camera