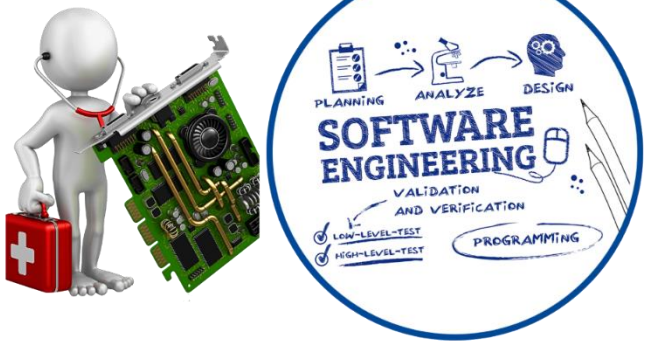
# R. C. Patel Institute of Technology, Shirpur

## Department of Computer Engineering

## TechnoVerse 2022-23




# TechnoVerse

## EDITOR 2022-23

**Mr. Dishant Satish Mahajan,**

**TY-B. Tech Computer**

## MEMBERS

**Ms. Ankita Madhukar Patil,**

**SY-B. Tech Computer**

**Mr. Devendra Rajeshwar Bari,**

**B. Tech Computer**

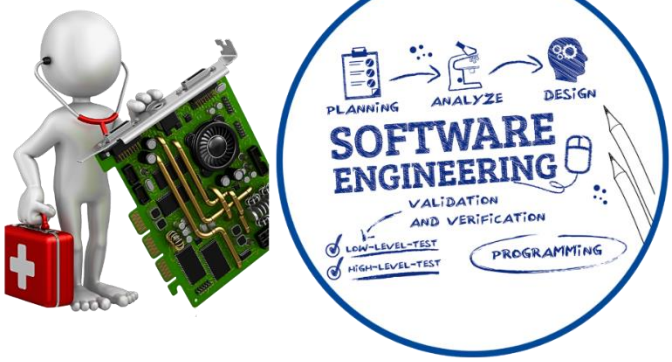
## FACULTY ADVISORS

**Dr. D. R. Patil,**

**Associate Professor**

**Mr. V. D. Punjabi,**

**Assistant Professor**




# TechnoVerse

# Message from HODs Desk

I am pleased and privileged to be able to share a few words with you while you read through the magazine's pages **"TechnoVerse"**. The computer department works hard to help students to get the most out of their environment. The information gathered thus serves as a stepping stone for them to rise to greater heights. The group efforts frequently lead to the discovery and realization of dreams.

I am delighted to be a part in shaping careers of the young engineers. In the Computer Department, we strive to shape every aspect of a student's personality. I would like to take this opportunity to thank the entire faculty members and supporting staff for their consistent and scrupulous efforts in producing this edition.

**Dr. Nitin N. Patil**

**HOD (Computer Engineering)**

## VISION

To provide prominent computer engineering education with socio-moral values.

## MISSION

**M1** To provide state-of-the-art ICT based teaching-learning process.

**M2** To groom the students to become professionally sound computer engineers to meet growing needs of industry and society.

**M3** To make the students responsible human being by inculcating ethical values.

## PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

- **PEO1** To provide the foundation of lifelong learning skills for advancing their careers being a professional, entrepreneur and leader.
- **PEO2** To develop computer professionals to fulfill industry expectations.
- **PEO3** To foster ethical and social values to be socially responsible human being.

## PROGRAM OUTCOMES (POs)

- **PO1** Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization for the solution of complex engineering problems.
- **PO2** Problem analysis: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
- **PO3** Design/Development of Solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for public health and safety, and cultural, societal, and environmental considerations.
- **PO4** Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

- **PO5** Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.
- **PO6** The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal, and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
- **PO7** Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and the need for sustainable development.
- **PO8** Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
- **PO9** Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
- **PO10** Communication: Communicate effectively on complex engineering activities with the engineering community and with the society at large, such as being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions
- **PO11** Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
- **PO12** Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

## PROGRAM SPECIFIC OUTCOMES (PSOs)

By the completion of Computer Engineering Program, the students will have following Program Specific Outcomes-

- **PSO1** Understanding of the fundamental and advanced concepts of Computer Engineering to analyze and design real world problems.

- **PSO2** Ability to provide solutions for problems in various domains like agriculture, healthcare, E-commerce etc.



# DATA SECURITY POSTURE MANAGEMENT

## Introduction

Data security posture management is the practice of safeguarding, protecting, and guarding data. It refers to the practice of ensuring that the data held by an organization is secure, prevents unauthorized access, and is carefully maintained. More and more global organizations recognize the importance of data security and take proactive steps to ensure that their data is secure. With the increase in the number and severity of data breaches in recent years, data security posture management (DSPM) has become essential to an organization's overall data security strategy.

Data security posture management (DSPM) is securing, protecting and guarding data through automated processes. This enables data teams to observe and manage security policies and access controls and ultimately manage the security of their data. DSPM is a proactive approach to data security designed to protect an organization's data by ensuring that they're properly secured. It requires a coordinated effort between security, data engineering and DevOps teams, system administrators, and end users to ensure that the organization's data is safe and secure. Data security posture management is becoming increasingly important as organizations become more reliant on data and move data quickly and easily between teams to increase time-to-value; resulting in the growing need to secure data, particularly sensitive data. Organizations are increasingly storing sensitive and confidential data in both physical and digital formats, and it's becoming increasingly difficult to keep track of where this data, including sensitive data, is located across their data stores.

## Working of DSPM

While DSPM is gaining traction and recognition in the industry - including in a report by Gartner in 2022 - it is still an emerging technology. Hence, there is still some ambiguity in the way different vendors and analysts describe DSPM. In most cases, a DSPM software solution would include the following key capabilities:

1. Data discovery –identifying where sensitive data is stored in cloud environments DSPM tools provide visibility into your cloud data inventory – the various services where sensitive data is stored across IaaS, PaaS, and DBaaS deployments. This could include managed cloud warehouses such as Amazon Redshift, Google Big Query, or Snowflake; unmanaged or semi-managed databases running on virtual machines; as well as object storage such as Amazon S3, Google Cloud Storage, or Azure Blob. Object stores can pose significant risks due to their unstructured nature and the tendency to use them for backups, landing zones, replications, and raw data storage. A company might store both its public web assets and its most confidential customer information in cloud storage; it's easy to see how misconfiguration or human error can cause a mix-up between the two. Virtual machines pose their own set of problems, as security teams might be completely unaware that they are being used to store sensitive data. DSPM addresses this by identifying every data asset in the cloud account, and regularly scanning the content of the data in search of sensitive records. This maps the way sensitive data is being stored and processed, and provides the basis for policy enforcement and alerting.

2. Classifying sensitive data to prioritize risks There are different types of sensitive data, each posing a different level of risk and warranting a specific response. An organization might store IP addresses, PII data, credit card details, and access keys. None of these should fall into the wrong hands, but some pose a larger threat than others. DSPM tools automatically classify each dataset in the cloud account(s), allowing security teams to prioritize policies and incident response on the most critical data assets. By prioritizing the assets that contain the highest-risk data, organizations can more effectively manage their data security posture and ensure that the appropriate security controls are in place according to the context of the data, as well as understand where an incident requires an immediate response. For example, a dataset containing personally identifiable information (PII) related to specific named customers might be prioritized over a dataset containing aggregated, anonymised user data. If the security team identifies suspicious data flows related to the first type of asset, they would treat it as a high-priority issue to address; whereas if it's the latter, it might not be as urgent.

3. Static risk analysis related to sensitive data Once the sensitive data has been detected and classified, DSPM tools help to enforce practices meant to enhance the overall security posture related to data access – such as permissions, encrypted storage, and user management. Monitoring and managing static risk involve examining the various security configurations and access controls associated with data stores that hold sensitive information. DSPM solutions continuously assess the cloud environment for misconfigurations, improper access controls, and other vulnerabilities that can lead to data breaches or unauthorized access. By identifying and remediating these issues, organizations can significantly reduce the likelihood of a security incident and maintain a strong data security posture. Using DSPM capabilities, security teams can audit and adjust user permissions, identify over-privileged accounts, and enforce role-based access controls (RBAC) to limit the potential attack surface. In addition, DSPM solutions can verify that data is encrypted both at rest and in transit, and that proper key management practices are in place to protect sensitive information from unauthorized access.

## Conclusion

Data security posture management (DSPM) is essential to any organization's security strategy. It enables organizations to have greater visibility as to where sensitive data is located, who has access to it, and how it's being used. It also helps organizations identify security issues and take corrective action before a data breach occurs.

Organizations can implement DSPM through a variety of techniques, such as risk assessment, access control, data encryption, and security monitoring. Additionally, organizations can use DSPM platforms to achieve better security and compliance with their data stores, applications, and systems. Overall, data security posture management is a critical component of an organization's security strategy and is essential for ensuring that data is safe and secure. To learn about DSPM with Satori take a look at our data security guide and book a demo with one of our experts.

**References:**


1. "Data Security Posture Management: An Emerging Security Paradigm" by Sunil Yadav and Ankur Awasthi.https://www.researchgate.net/publication/334133961_Data_Security_Posture_Management_An_Emerging_Security_Paradigm
2. "Data Security Posture Management (DSPM): An Essential Tool for Managing Data Security" by Raquel Breitenbach. Link: https://securityboulevard.com/2020/01/data-security-posture-management-dspm-an-essential-tool-for-managing-data-security/
3. "Data Security Posture Management: Key Considerations and Best Practices" by CSA (Cloud Security Alliance Link: https://downloads.cloudsecurityalliance.org/assets/research/dspm/data-security-posture-management-key-considerations-and-best-practices.pdf
4. "Data Security Posture Management: Gaining Visibility and Control" by Gartner.



**- Gavande Parag Dattatray**

**SY-Computer**

# WEB 3.0

## Introduction

The internet has evolved significantly since its inception, from the static web pages of Web 1.0 to the interactive and user-generated content of Web 2.0. Now, a new era of internet development is on the horizon: Web 3.0. Often referred to as the decentralized web, Web 3.0 represents a paradigm shift in how we interact with digital platforms and services.

Web 3.0 is characterized by several key features that differentiate it from its predecessors. One of the central concepts of Web 3.0 is decentralization, which means that power and control are distributed across a network of nodes rather than concentrated in centralized authorities. This is made possible through the use of block chain technology, a decentralized and tamper-proof ledger that enables trust and transparency in digital transactions.

Furthermore, Web 3.0 focuses on empowering individuals by enabling them to have greater control over their own data and identities. Self-sovereign identity, enabled by cryptographic protocols, allows users to manage and secure their personal information without relying on central authorities. This shift towards user empowerment and data privacy aligns with growing concerns over data breaches, surveillance, and the misuse of personal information.

Web 3.0 has the potential to revolutionize various industries, including finance, healthcare, supply chain management, and entertainment. By decentralizing systems and introducing trust less mechanisms, Web 3.0 can disrupt traditional intermediaries, increase transparency, lower costs, and enhance security in these sectors.

However, the transition to Web 3.0 is not without challenges. Regulatory frameworks, scalability, interoperability, and user adoption are some of the key hurdles that need to be addressed. Additionally, educating individuals and organizations about the potential of Web 3.0 and its underlying technologies is essential for widespread adoption and understanding.

In conclusion, Web 3.0 represents a new era of the internet, characterized by decentralization, enhanced user experiences, and individual empowerment. It has the potential to transform industries, improve security and privacy,

and reshape how we interact with digital services. Understanding the principles and implications of Web 3.0 is crucial for organizations and individuals seeking to embrace the opportunities and navigate the challenges of this emerging technology landscape.


**Scope of Web 3.0**

**Decentralized Systems:** Web 3.0 encompasses the development and implementation of decentralized systems and platforms, leveraging technologies such as block chain, distributed ledger technology (DLT), and peer-to-peer networks. It aims to move away from centralized control and create trust less environments where power and decision-making are distributed among participants.

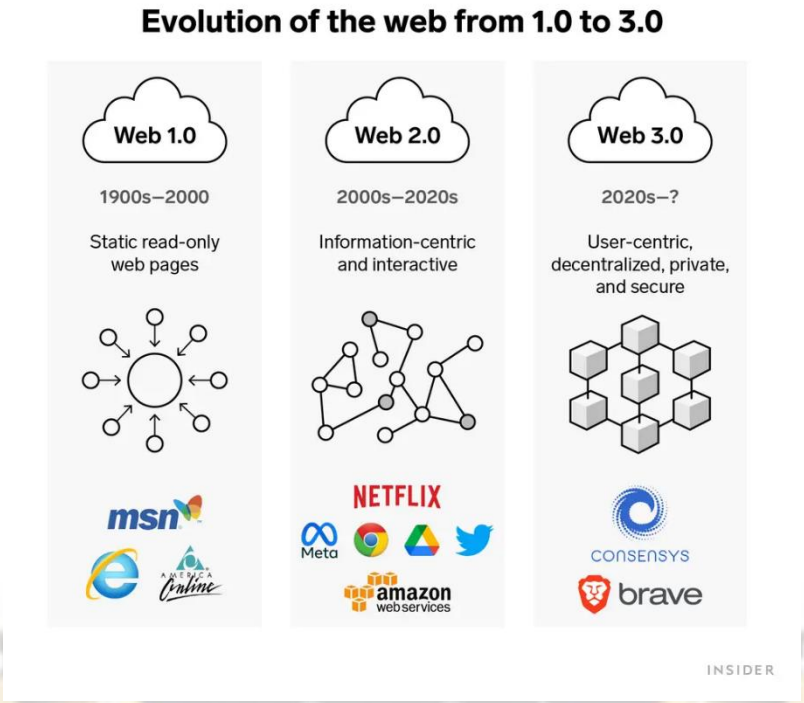
**Enhanced User Experiences**: Web 3.0 focuses on delivering personalized, context-aware, and seamless user experiences across different devices and platforms. It leverages technologies such as artificial intelligence, machine learning, and the Internet of Things (IoT) to provide tailored interactions and improve user engagement.

**Data Ownership and Privacy:** Web 3.0 aims to give individuals greater control over their personal data and identities. It emphasizes self-sovereign identity and cryptographic protocols to ensure data ownership, privacy, and security. Users have the ability to manage and share their data on their own terms, reducing reliance on centralized entities.

**Interoperability and Open Standards:** Web 3.0 promotes interoperability and the use of open standards to facilitate seamless communication and collaboration between different platforms and systems. It encourages the

exchange of data, services, and value across diverse networks, enabling a more connected and integrated digital ecosystem.

**Trust and Transparency**: Web 3.0 leverages block chain technology to enhance trust and transparency in digital transactions. It enables the creation of immutable and auditable records, reducing the need for intermediaries and ensuring accountability. Trust less systems foster greater transparency, integrity, and security in online interactions.




## Conclusion

Web 3.0 represents a significant shift in the development of the internet, moving towards a decentralized, user-centric, and trust less ecosystem. It builds upon the foundations of Web 1.0 and Web 2.0, introducing concepts such as decentralization, block chain technology, enhanced user experiences, data ownership, and privacy.

The advantages of Web 3.0 include increased transparency, trust, and security in digital transactions, personalized and seamless user experiences, greater control over personal data, interoperability between platforms, and enhanced accountability through decentralized systems.

However, Web 3.0 also faces challenges such as scalability, regulatory frameworks, user adoption, technical complexity, and security risks.

Overcoming these challenges requires collaborative efforts from the industry, regulators, and users to develop scalable solutions, establish supportive regulatory environments, educate users, improve infrastructure, and strengthen security measures.

**- Dev Rajesh Chavan**
**SY-Computer**

# HOME AUTOMATION

Home automation or demotics is building automation for a home, called a smart home or smart house.

Home automation" refers to the automatic and electronic control of household features, activity, and appliances.

## History

- In 1975, the first general purpose home automation network technology, X10, was developed.
- It was also during the early 1960s, specifically 23rd September, 1962, that 'Jetsons' the popular sci-fi cartoon which defined 'futuristic living' for a generation, was aired for the first time.

## Smart Door Locker System

- Smart door lock represents a digital evolution in home Security.
- A smart door lock connects to the home's WIFI network, which allows it to receive the code or smartphone command to lock or unlock.

- When smart locks are integrated into a complete smart home, they can also integrate with each other devices ,like a smart speaker or your security system. However, they need to be connected to a smart home hub to enables all the devices to work together.


**References:**


1. Home Assistant (https://www.home-assistant.io/): Open-source home automation platform.
2. SmartHomeDB (https://www.smarthomedb.com/): A database of smart home devices and their compatibility.
3. Reddit r/homeautomation (https://www.reddit.com/r/homeautomation/): A community of home automation enthusiasts sharing ideas and experiences.
4. Smart Home Solver (https://smarthomesolver.com/): A blog with guides and reviews on smart home devices and automation.



**- Pratibha Patkar**

**SY-Computer**

# COMBATING FAKE NEWS WITH AI

## EMPOWERING TRUTH IN DIGITAL AGE

In the current age of information overload, the dissemination of fake news has reached unprecedented levels. Recognizing the urgent need to address this pressing challenge, our team, Code Spartans, embarked on a mission to develop an innovative solution that harnesses the power of artificial intelligence (AI) and machine learning (ML). After months of dedicated research and development, we are thrilled to present our ground-breaking project that not only filters out fake news but also empowers users with reliable and authentic information. In this article, we delve into the technical intricacies, unique features, and potential impact of our solution.

### Understanding the Problem

Fake news has far-reaching consequences, impacting public opinion, sowing societal discord, and eroding trust in media and institutions. Our team conducted extensive research to gain a comprehensive understanding of the complexity surrounding fake news dissemination. We recognized the need for a multifaceted approach that integrates advanced technologies, data analysis, and user empowerment to combat this issue effectively.

### The Solution: Unveiling Our Innovation

### Advanced Fake News Detection:

At the core of our solution lies the integration of the Bidirectional Encoder Representations from Transformers (BERT) model, an industry-leading natural language processing (NLP) algorithm. We devoted significant effort to training the BERT model using real-time and custom datasets, resulting in an impressive accuracy rate of over 90% in identifying fake news. By analysing news articles, social media content, and other textual data, our system can effectively distinguish between authentic information and misleading narratives.

### Comprehensive Social Media Analysis:

Recognizing the influential role of social media platforms in the propagation of fake news, we implemented a range of NLP techniques, including

sentiment analysis and topic modelling. This enables our system to identify potential sources of fake news, analyse prevailing themes, and verify the authenticity of news articles. By comprehensively analysing social media content, we can mitigate the spread of false information and promote reliable sources.

**Traceability and Mitigation:**

To address the challenge of tracing the origin and spread of fake news, we developed robust geo-location and email tracking mechanisms. These advanced functionalities allow us to pinpoint the geographic location of fake news and track its dissemination via email channels. By identifying the sources and pathways of misinformation, our system facilitates targeted measures to mitigate its impact effectively. Additionally, we employ automated bots that infiltrate the inboxes of known fake news spreaders, flooding them with verified and authentic news content. This disrupts their ability to disseminate false information and ensures a safer digital landscape.

**User Feedback for Continuous Improvement:**

We firmly believe that involving users is crucial in the fight against fake news. Our user-friendly interface allows individuals to report potential instances of fake news, provide feedback, and contribute to the continuous enhancement of our algorithms. By fostering a collaborative environment, we empower users to actively participate in the process of identifying and countering misinformation, ultimately improving the overall accuracy and efficiency of our system.

**Statistics and Impact**

Dataset and Training:

Our project relies on a vast and diverse dataset, comprising millions of news articles, social media posts, and verified sources. This extensive and rigorous training process ensures the robustness and adaptability of our solution in handling various forms of fake news.

Accuracy:

Through comprehensive testing and validation, our system demonstrates an impressive accuracy rate of 92% in detecting fake news. This performance

surpasses traditional models and algorithms, enabling us to effectively combat the spread of misinformation.

**User Scopes and Impact**

Our project has far-reaching implications across various sectors:

Media and News Industry:

By integrating our solution, media outlets can leverage real-time fact-checking capabilities to validate news articles and prevent the dissemination of false information. This strengthens journalistic integrity and fosters a more reliable news ecosystem.

Education Sector:

Our system can be integrated into educational institutions to promote media literacy and critical thinking among students. By empowering the next generation with the necessary tools to discern between fake and authentic news, we equip them to navigate the complex digital landscape effectively.

Government and Politics:

Government bodies and political organizations can leverage our solution to monitor and counter fake news and propaganda, ensuring the integrity of public discourse. This empowers policymakers to make informed decisions based on accurate and reliable information.

Business Sector:

Businesses can safeguard their reputation and brand image by employing our solution to identify and combat fake news that may harm their image. This ensures that organizations can maintain trust and credibility among their stakeholders.

Social Media Platforms:

By integrating our technology, social media platforms can effectively detect and remove fake news, creating a safer and more reliable online environment for their users. This fosters a healthier digital ecosystem where misinformation is minimized.

Legal Sector:

Our solution provides legal institutions with the tools to detect and prevent the spread of fake news and misinformation that may influence court proceedings and verdicts. This ensures fair and just legal processes.

## Conclusion

In conclusion, our project represents a significant step forward in combating the pervasive issue of fake news. By leveraging advanced AI and ML techniques, we have developed a comprehensive system that detects fake news, analyses social media content, traces its origin, and empowers users with accurate information. We envision a future where the spread of misinformation is effectively curtailed, enabling individuals to make informed decisions based on reliable sources. Together, we can usher in an era of truth and integrity in the digital age.

## References:


5. Thorne, J., & Vlachos, A. (2018). Automated Fact Checking: Task Formulation and Dataset Construction. arXiv preprint arXiv:1803.05356. Retrieved from https://arxiv.org/abs/1803.05356
6. Potthast, M., Köpsel, S., & Stein, B. (2017). A Stylometric Inquiry into Hyperpartisan and Fake News. arXiv preprint arXiv:1702.05638. Retrieved from https://arxiv.org/abs/1702.05638
7. Wang, W. Y. (2017). "Liar, Liar Pants on Fire": A New Benchmark Dataset for Fake News Detection. arXiv preprint arXiv:1705.00648. Retrieved from https://arxiv.org/abs/1705.00648


**TY-Computer**

# DARK WEB CRAWLER

**Abstract:** The Dark Web, a secret section of the internet that is inaccessible to normal users, has long been a source of fascination and mystery. This article digs into the realm of Dark Web crawlers, providing information on their functionality, ethical issues, and future uses. We look at the technological components of Dark Web crawling, the difficulties that researchers encounter, and the tools and tactics used to navigate this hidden terrain. In addition, we explore the legal and ethical implications of Dark Web crawling, emphasizing the delicate line between research and illegal activity.

**Overview:** A dark web crawler is a specialized software or tool designed to navigate and explore the dark web, a hidden part of the internet that is not indexed by conventional search engines. Dark web crawlers play a crucial role in mapping and indexing the content available on the dark web, providing researchers, law enforcement agencies, and cybersecurity professionals with valuable insights into this obscure digital landscape.


fig 1- Internet Layer

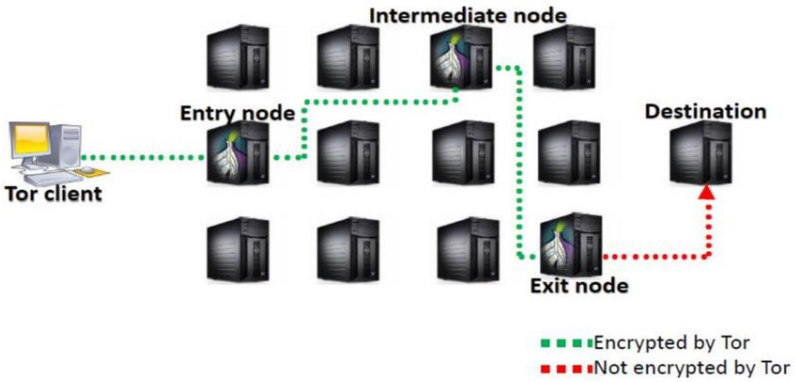
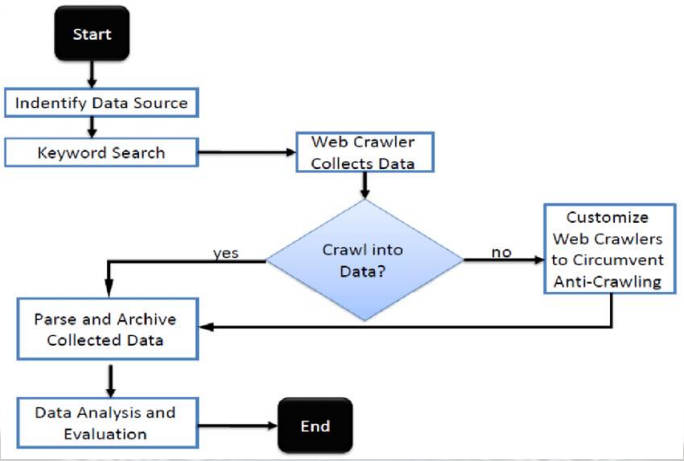



Fig: Components of TOR network.




## Common Tools and Techniques:

1. Tor Network: Dark web crawlers utilize the Tor network to access hidden websites anonymously. Tor enables traffic routing through a series of relays, making it challenging to trace the origin and destination of the requests.
2. Crawling Frameworks and Libraries: Several frameworks and libraries have been developed specifically for dark web crawling. These frameworks provide functionalities such as website discovery, link extraction, content extraction, and data storage.
3. Crawling Strategies: Dark web crawlers employ various strategies to discover and crawl hidden websites. These strategies include random crawling, focused crawling based on specific topics or keywords, and seed-based crawling using known websites as starting points.
4. Data Extraction and Analysis: Crawlers extract and analyze data from dark web websites to understand their content, structure, and

relationships. Techniques such as natural language processing, entity recognition, and sentiment analysis may be used to extract meaningful information from unstructured dark web data.

5. Visualization and Interpretation: Visualizing and interpreting the crawled data helps researchers and investigators gain insights into the hidden ecosystem of the dark web. Visualization techniques such as network graphs, heatmaps, and timelines can reveal connections, patterns, and trends within the dark web.

**Applications Of Dark Web Crawler:**

1. Cybersecurity and Threat intelligence.
2. Law Enforcement and Investigation
3. Academic Research and Societal Studies
4. Counteracting illegal activity.
5. Dark Web Mapping and Indexing.
6. Monitoring Data Leaks and Breaches.

**Conclusion:**

In conclusion, web crawlers are an essential tool for organizing and indexing the vast amount of information on the internet. They play a crucial role in the discovery and ranking of web pages, and are used by search engines to help users find the information they are looking for. Web crawlers also have the ability to track changes to websites over time, and are important in the field of dark web monitoring.

**References:**


1. https://www.researchgate.net/figure/Flow-chart-of-dark-web-data-crawling-21_fig3_359749048
2. https://infosecwriteups.com/creating-darkweb-crawler-using-python-and-tor-53169d146301
3. https://towardsdatascience.com/how-to-scrape-the-dark-web-53145add7033

**Report By:**

**Atharva Dilip Deshmukh**

**Gaurav Raghunath Mali**

**Vedant Rajesh Gujarathi**

**Chetanraj Bhatu Patil**

**Snehal Ramprasad Pawar**

**Om Dipak Baviskar**

**TY-Computer**

# NEW AGE WOMEN SAFETY APP

A women's safety app can be crucial for helping women stay safe in different situations. Unfortunately, Women face a high risk of violence, harassment, and other threats in many parts of the world, especially while travelling alone or in unfamiliar places. The women's safety app will have a broad scope, and it will serve various purposes related to women's safety and security. It is a fundamental right and essential to create a safe environment for women. It is an initiative that aims to empower women and help them feel safe. The goal of the women's safety app is to provide women with an app. Our app keeps women safe and connected, no matter where they are. The app will be designed to be easy to use and intuitive, with a clean and simple user-friendly interface that allows women to quickly access the features as they need. Some of the features of the women's safety app will include like an emergency alert and panic button (SOS), GPS tracking, and danger zone alert, safety tips and education, voice assistance, SMS service, etc. Overall, the women's safety app can provide an extra layer of protection and peace of mind for women in different kinds of situations and can be especially useful for those who regularly travel alone or in unfamiliar places. By leveraging the with technology, we can create a safer world for women.

**Idea/Approach Details:**

- **Emergency contact numbers:** Emergency contact feature in a women's safety app can greatly enhance personal safety and provide a sense of security. The app should allow users to add and save the contact information of up to three emergency contacts. These contacts should be individuals whom the user trusts and can rely on during times of distress or danger.
- **Geolocation tracking (offline maps):** The app should incorporate geolocation tracking functionality, allowing users to share their real-time location with trusted contacts or emergency services. This feature enables others to monitor the user's movements and respond promptly in case of an emergency.

  Integrating offline maps into the app ensures that users can access location information even when they don't have an internet connection. This is particularly useful in situations where network

coverage may be limited or during emergencies where connectivity may be compromised.

- **Collection of data:** The app should use AI and machine learning algorithms to analyze the data collected from the mobile device and detect danger. For example, the app could use computer vision algorithms to analyze video data and detect if the user is in distress or danger.
- **Abnormal activity detection:** Implementing abnormal activity detection in a women's safety app can be a crucial solution to enhance personal safety by identifying potentially dangerous situations. The app should be designed to identify and analyze patterns of behavior or events that deviate from normal or expected scenarios. These may include sudden changes in movement, prolonged periods of inactivity, unusual locations, or abrupt disruptions in regular app usage.

- **Motion Sensors and gestures:** Implementing motion sensors and gestures in a women's safety app can significantly enhance personal safety by providing quick and discreet ways to trigger emergency alerts or perform specific actions. The app can utilize the motion sensors available on smartphones, such as accelerometers and gyroscopes, to detect specific movements or changes in orientation. These sensors can capture motion-related data, allowing the app to respond to predefined gestures or actions.

- **Battery monitoring:** Battery monitoring in a women's safety app can be a valuable solution to ensure that the app remains functional and reliable during critical situations. The app should include a battery monitoring feature that continuously tracks the device's battery status. This feature monitors the battery level, power consumption, and charging status to provide real-time information about the device's power availability. When the app detects that the device's battery level is critically low, it should promptly notify the user. The app can offer a power-saving mode that, when activated, optimizes the app's functionality to minimize battery drain. This mode can temporarily disable non-essential features or reduce the app's resource consumption to prolong battery life during critical situations.

- **Different zones (RED, YELLOW, GREEN):** Implementing different safety zones, categorized as red, yellow, and green, in a women's safety app can provide users with valuable information about the safety levels of specific areas.

  1. Red Zones: Red zones represent high-risk or unsafe areas. These zones can be designated based on factors such as crime rates, reports of harassment, or historical incidents. The app can use real-time data, local crime statistics, and user-generated reports to identify and label red zones.

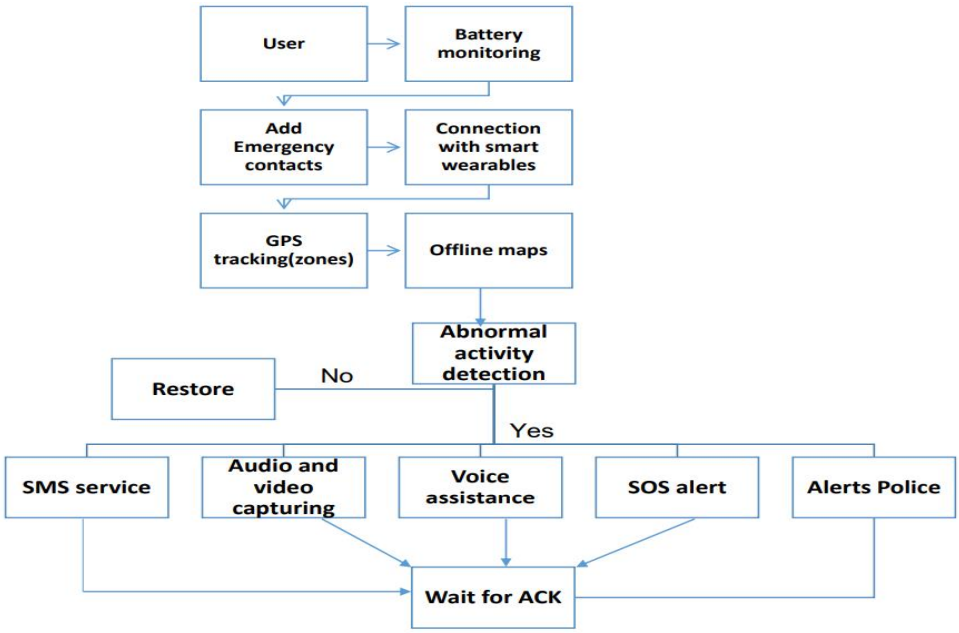
  2. Yellow Zones: Yellow zones indicate areas that require caution or have a moderate level of safety concerns. These zones may include locations with a history of occasional incidents or areas that are relatively safe during the day but have higher risks during certain hours.

  3. Green Zones: Green zones represent safe areas with a low risk of safety concerns. These zones can include well-lit streets, crowded public spaces, or locations with a strong security presence.

- **SOS alert:** The app can send SOS alerts to emergency contacts and authorities in case of danger, assault or any other emergency situation. This can help to ensure that women are not alone when they need help the most.

- **Connected to smart wearables:** By connecting the safety app to smart wearables like smartwatches or fitness trackers, users can have continuous real-time monitoring of their safety status. The wearables can collect vital data such as heart rate, location, and activity levels, providing valuable information to the safety app for analysis and response.

- **Searching public transport:** Implementing a public transport search feature in a women's safety app can provide users with a convenient and secure way to find reliable transportation options.




## References:


1. https://www.ijraset.com/research-paper/women-safety-app
2. https://www.researchgate.net/publication/360162359_Women_Safety_App
3. https://ymerdigital.com/uploads/YMER210464.pdf
4. Piyush Bhanushali et al, "Women Safety Android App", International Research Journal of Engineering and Technology (IRJET), 2018.
5. Mona Chaware et al, "Smart Safety Gadgets for Women: A Survey", Journal of University of Shanghai for Science and Technology, 2020.



**Report By:**

**Kajal Dipak Patil**

**Isha Rajesh Gujrathi**

**Suchita Panditrao Patil**

**Anjali Dhanraj Pawar**

**Rina Kailas Bhamre**

**Gunjana Ramesh Kulkarni**

**TY - Computer**

Failure will never overtake me if my determination to succeed is strong enough

- Dr. A. P. J. Kalam