Incorporating Dark Web Education into Cybersecurity Curricula

Zouheir Trabelsi
College of Information Technology
United Arab Emirates University
Al Ain, UAE
Trabelsi@uaeu.ac.ae

Firas Saidi
University of Technology Bahrain
Salmabad, Bahrain
firassaidi@yahoo.fr

Ban Alomar
College of Information Technology
United Arab Emirates University
Al Ain, UAE
700039223@uaeu.ac.ae

Tariq Qayyum
College of Information Technology
United Arab Emirates University
Al Ain, UAE
700036923@uaeu.ac.ae

2025 IEEE Global Engineering Education Conference (EDUCON) | 979-8-3315-3949-8/25/$31.00 ©2025 IEEE | DOI: 10.1109/EDUCON62633.2025.11016356

***Abstract*—The Dark web is considered the concealed part of the internet and harbors a huge assortment of cyber threats that compromise global security. One must understand what goes into the technical infrastructure of the Dark Web to develop an effective strategy for monitoring threats, conducting investigations, and implementing the appropriate security measures necessary to protect against illegal activities and data breaches originating from the Dark Web. In such a rapidly changing cyber threat landscape, especially threats originating from the Dark Web, it calls for a re-evaluation of the traditional information security curricula at academic institutions. This educational research work investigates the compelling need to integrate Dark Web Education into Cybersecurity programs for arming the future workforce with a comprehensive knowledge base and skillset necessary to fight modern-day cyber threats. A review of the current state of cybersecurity education reveals wide gaps in knowledge and readiness about Dark Web issues. This paper presents a structured approach for integrating Dark Web topics into the existing curricula on cybersecurity, focusing on legal, ethical, and technical dimensions. We believe in balance: on one side, theoretical knowledge; on the other, hands-on experiences that ensure the learner takes away just how complex the Dark Web is—without taking part in or condoning any illegal activities. Equally, a set of recommendations are commented on for educators and developers of curricula to integrate education about Dark Web safely and effectively into their cybersecurity programs, which will enhance the overall quality and relevance of cybersecurity education in preparing the students for the challenges of the digital age.**

***Index Terms*—Dark Web, Deep Web, Information security curricula, Cybersecurity, Ethical hacking.**

I. Introduction

The terms Darknet and Dark Web refer to distinct, though related, concepts in the broader context of the Internet and hidden online activity. The Darknet is a network built on top of the existing Internet but requires specific software, configurations, or authorization to access. It functions as an overlay network that is not indexed by standard search engines, like Google and Bing, and is used for maintaining privacy and anonymity. The most well-known Darknet is Tor (The Onion Router), which allows users to browse the Internet anonymously. Others include I2P (Invisible Internet Project) and Freenet. Darknets are often used for secure, private communications, activism under oppressive regimes, or by whistleblowers. However, they are also sometimes used for illicit activities due to their anonymizing features. The Dark web is a subset of the Deep web, which consists of content that is not indexed by traditional search engines [1]. The Dark web specifically refers to sites and content that exist on Darknets and require special software, such as the Tor browser, to visit Dark web sites, which often have the '.onion' domain suffix. While the Dark web is part of the Deep web (all parts of the Internet not indexed by search engines), not all of the Deep web is dark. For example, content like password-protected sites or academic databases are part of the Deep web but are not considered part of the Dark web. In summary, the Darknet refers to the underlying network that allows for anonymous communication and browsing, while the Dark web is the content and sites that exist within those networks.

Despite its legitimate uses, the Dark web is fraught with risks. It is a heaven for criminal activities, which include the trafficking of drugs, weapons, and stolen data. One can also encounter harmful software, such as malware and ransomware. Its encrypted nature means that law enforcement and government agencies find it hard to monitor and tackle illegal activities. Users are advised to be conscious of the legal consequences of their actions online and to be informed of the risks and responsibilities involved in accessing the Dark Web. With its positive side as a useful tool for privacy advocates, the Dark Web seriously brings along ethical, legal, and security concerns [2].

In contrast, knowledge of the technical underpinning of the Dark Web becomes an essential requirement for cybersecurity practitioners in devising related strategies for threat monitoring, conducting investigative activities, and implementing appropriate security measures to protect against malicious operations and data breaches emanating from this hidden part of the Internet [3], [4]. Besides, as the dark web's influence on society is increasing, it is reasonable to assume that educational programs and public awareness campaigns will discuss its dynamics and consequences, thus creating a wiser and better-prepared audience [5].

This educational research project points out the necessity to include Dark web studies in cybersecurity curricula for empowering future cybersecurity professionals with broad knowledge and the necessary skills to deal with modern cyber threats. It also provides a structured approach toward integrating Dark web topics into the existing courses of cybersecurity, which are presented from a legal, ethical, and technical perspective. A comprehensive strategy that integrates theoretical insights with experiential learning opportunities is presented, facilitating students' comprehension of the intricacies associated with the Dark web while refraining from participation in or endorsement of unlawful actions. Some tips are given for educators and curriculum developers to safely and effectively include Dark Web education in their cybersecurity programs in order to make the cybersecurity education more relevant and effective for preparing students to handle challenges presented by the digital era.

The remainder of the paper is organized in the following manner: Section 2 presents the identified knowledge gaps in current offered cybersecurity curricula concerning the Dark Web topics. Section 3 discusses the need for Dark Web education. Section 4 outlines the integration of Dark Web topics into cybersecurity courses. Section 5 lists learning objetives and outcomes related to the Dark Web. Section 6 proposes a structured outline of a module on Dark Web. Section 7 discusses the design and development of hands-on lab activities on Dark Web. Section 8 discuses Artificial Intelligence (AI) based hands-on labs. Section 10 proposes a set of quiz questions on Dark Web and cryptocurrencies to asset student's performance. Finally, Section 11 concludes the paper.

II. Knowledge Gaps Concerning the Dark Web

The current landscape examination of information security education reveals that there are significant gaps in knowledge and preparedness concerning the Dark Web.

A. *Publications on Dark Web Education*

The inclusion of topics related to the Dark web in academic curricula has drawn attention in recent years, although the number of academic papers dealing explicitly with this issue remains limited.

In [3], the authors put to fore the importance of including Dark web research as part of criminal justice curriculum, even suggesting course and syllabi resources. However, the suggested syllabus is mainly designed for those who are majoring in criminal justice and not cybersecurity majors taking courses with computer science background.

In [6], authors' investigated a research study that examines the valid integration of topics related to the Deep web and Dark web into higher education curriculums. This manuscript provides a critical perspective for educators to integrate Dark web instruction responsibly, and highlights the need for preparing the student body to face real-world challenges in cybersecurity. The authors of this paper stress the increasing importance of the Deep web and Dark web in cybercrime, data breaches, and other illicit activities, and insist on the fact that these topics be introduced within the curricula of cybersecurity and criminal justice programs at all higher education institutions. This study also provides a framework for creating a course or module on the Deep web and Dark web, including clear objectives, likely challenges, and recommended content areas. These publications indicate an increasing awareness of the need for Dark Web education, especially in fields such as criminal justice and cybersecurity. The total number of academic publications on this subject remains comparatively few, however.

B. *Cybersecurity Courses on Dark Web*

The Dark web cybersecurity classes generally are offered by institutions having strong programs in either cybersecurity or criminal justice. Not very many are actually covering Dark web topics in-depth as part of broader subjects like cyber threats, network security, digital forensics, ethical hacking, and cybercrime investigation. Programs requiring pre-existing foundational knowledge in cybersecurity or computer science may also include associated hands-on lab components or research on monitoring and analyzing the Dark web.

A number of academic institutions in the United States are noted for offering programs that deal with the technical, legal, and ethical aspects of the Dark web, preparing students for careers in cybersecurity, law enforcement, and intelligence that require specialized knowledge of activities related to the Dark web and related mitigation measures.

Carnegie Mellon University (CMU) offers special courses in the study of cyber intelligence and Dark Web analysis through its CyLab Security and Privacy Institute. The University of California, Berkeley, via its School of Information, has courses on cybersecurity and privacy that cover the Dark Web sporadically in the context of cybercrime.

The Tandon School of Engineering at New York University provides educational opportunities in cybercrime investigations, digital forensics, and analysis of the Dark Web within its cyber studies curriculum, thereby preparing students with essential investigative competencies. Subjects like cybercrime, forensics, and Dark Web studies were part of Purdue University's Computer and Information Technology Department's Master's in Cybersecurity and Network Engineering program. The Viterbi School of Engineering at the University of Southern California also teaches classes in cyber intelligence and forensics, which includes coursework on the Dark Web. Rochester Institute of Technology's (RIT) cybersecurity coursework also includes classes in both Dark Web research and digital forensics for undergraduate and graduate students. Norwich University offers several online programs in cybersecurity, including cybersecurity of the Dark Web and cyber intelligence, providing flexibility for remote students. Among a few other universities, the University of Maryland, Global Campus, does offer a Master's degree in Digital Forensics and Cyber Investigation; coursework includes monitoring the Dark Web. The University does focus more on hands-on skills in digital forensics.

George Mason University (GMU) has a dedicated course, Exploring the Darknet (DFORS 780) [7], introducing students to the distinctions between the Darknet and Surface Web, covering components and protocols, and examining Tor Browser's role in anonymous web browsing. The course further explores how cybercriminals and nation-states utilize the Darknet, and the efforts law enforcement takes to deanonymize criminal activities. Additionally, GMU offers a second course titled Darknet Technologies (DFOR 780) [8], with an initial focus on the Darknet followed by a deep dive into its underlying technologies. Ferris State University developed an Information Security and Intelligence program, a grant-funded curriculum emphasizing social media and Dark Web analysis, preparing students for careers in computer forensics, information security, ethical hacking, penetration testing, big data intelligence, incident response, and mobile security [9]. In [3], a survey of two- and four-year colleges, in Texas, revealed that only one cybersecurity program included Dark Web or Darknet classes, indicating limited availability of such specialized courses in the region.

Moreover, a relatively limited number of academic institutions around the world offer training programs that lead to certificates on the Dark web. As an example, Georgia State University, USA, offers a three-day training course, that lead to a certificate, titled EBCS Certificate of Darknet Intelligence Collector and Investigator [10]. This course will equip students with the practical experience required for gathering intelligence from Darknet and encrypted online communication platforms, as well as compiling the data and analyzing it in a way which will support any operation. In addition, this course will prepare students for accessing and findings Darknet markets and forums over several platforms, and facilitate the skills required for engaging and developing rapport with online criminal actors. Moreover, the followings are two other examples of institutions around the world providing specialized courses or modules related to the Dark web. Charles Sturt University, School of Computing and Mathematics, Australia, offers a course on Dark net, ITC578 Dark Web, to postgraduate students [11]. This course provides a broad overview of emerging digital threats and computer crimes, with an emphasis on cyber-stalking, hacktivism, fraud and identity theft, and attacks on critical infrastructure. The subject also analyses the online underground economy and digital currencies, and cybercrime on the Dark web.

Cyberlaw University, India, offers a course on Dark web, called Mystery of Darknet Law [12]. In this course, students will get a broad overview about Darknet wherein all kinds of criminal activities and acts are being done. In this course, students will also get to learn about the various practical legal policy and regulatory issues and challenges that the advent of Darknet is beginning to throw up. Students will also learn how the legal jurisprudence pertaining to Darknet is at a very early stage of its development, and how there is a need for coming up with appropriate innovative legal strategies and approaches so as to deal with the emerging legal challenges thrown up by the Darknet.

C. Cybersecurity Students Knowledge on Dark Web topics

In an effort to evaluate the student's basic knowledge on Dark Web topics, a questionnaire was given to 85 students who are enrolled in our university's information security program. The selected students were in their last graduation semester and did not receive any course, hands-on lab or educational materials on Dark web and cryptocurrencies during their study journey at our university. In the questionnaire, the students were asked to express their confidentiality level to answer a number of questions about the Dark web and cryptocurrencies. The following is the list of the questions:

- Q1: What are the differences between the Deep web, the Dark web, and the Surface web?
- Q2: What are the tools and software required to access the Dark Web?
- Q3: How hidden services are discovered in the Dark web?
- Q4: How user anonymity is maintained in the Dark Web?
- Q5: What kind of legal activities can be found on the Dark web?
- Q6: What are the ethical considerations of accessing and using the Dark web?
- Q7: What are the risks associated with using the Dark web?
- Q8: What are the common security measures one should take before accessing the Dark web?
- Q9: What is the primary reason cryptocurrencies are used on the Dark Web?
- Q10: Are cryptocurrency transactions on the Dark Web completely untraceable?
- Q11: How do cryptocurrencies maintain user anonymity?
- Q12: Which cryptocurrency is the most commonly associated with transactions on the Dark Web (Ethereum, Bitcoin, Ripple, Litecoin)?
- Q13: What is the major concern regarding the use of cryptocurrencies on the Dark Web (Speed of transaction, Exchange rates, Anonymity leading to illegal activities, High transaction fees)?

Table I shows the questions of the questionnaire and the frequencies of the students' responses. The responses are on a Likert-scale of 1 to 5, where 1 is "Not confident at all", 2 is "Not sure", 3 is "Light confident", 4 is "Confident", and 5 is "Strongly confident" to respond correctly a given question. The students' responses frequencies indicate clearly that more than 90% of the selected students were not confident at all or not sure about being able to provide correct responses to the questions. In addition, more than 80% of the students have very limited knowledge about the field of cryptocurrencies. Therefore, the questionnaire's results contribute to confirm the claim that the majority of the cybersecurity students have very limited or superficial knowledge on Dark web and cryptocurrencies topics.

TABLE I
SCALE RESPONSES FOR DARK WEB AND CRYPTOCURRENCIES RELATED QUESTIONS

Questions	Scale 1	Scale 2	Scale 3	Scale 4	Scale 5
Dark web related questions:					
Q1	50	28	5	2	0
Q2	45	34	4	0	2
Q3	47	33	2	0	3
Q4	35	46	2	0	2
Q5	30	30	17	4	4
Q6	52	25	7	1	0
Q7	47	33	2	0	3
Q8	35	46	2	0	2
Cryptocurrencies related questions:					
Q9	50	28	5	2	0
Q10	45	34	4	0	2
Q11	29	31	18	3	4
Q12	52	25	7	1	0
Q13	49	31	2	0	3

III. THE NEED FOR DARK WEB EDUCATION

The importance of Dark Web education for cybersecurity students is increasingly recognized as a critical element of comprehensive cybersecurity training. By incorporating this education into cybersecurity programs, institutions can equip students with essential knowledge, skills, and ethical considerations to navigate the complexities of modern cybersecurity challenges. This focus is not about endorsing Dark Web usage but rather understanding its impact on global security and privacy to develop robust defense mechanisms against associated threats [13], [14].

Understanding the Dark Web allows students to learn about the origins of various cyber threats and how they can be mitigated. By educating students on these aspects, they gain insights into the range of threats faced by organizations and become better equipped to assess risks.

The Dark Web relies on anonymity tools like Tor (The Onion Router), and educating students about these tools is essential not only for investigating and mitigating cyber threats but also for understanding online privacy concerns and legitimate anonymity uses. Additionally, the Dark Web can serve as a valuable source of cyber threat intelligence. Students can learn to monitor forums and marketplaces for leaked data, emerging malware, and cybercriminal discussions. This type of intelligence gathering informs security strategies and strengthens defensive measures [15].

In cybercrime investigations, familiarity with the Dark Web enhances a professional's ability to track and analyze cybercriminal activities, which is crucial for incident response and forensic investigations. Knowledge of how cybercriminals operate and the data and tools they utilize on the Dark Web enriches investigative techniques, making it invaluable for forensics analysts and incident responders.

IV. INTEGRATING DARK WEB TOPICS INTO CYBERSECURITY COURSES

Such integration of Dark web topics into cybersecurity courses will improve the students' understanding of the cyber threat landscape, thereby preparing them better for real-world challenges. Here are some discussions on how educators might effectively or successfully integrate the topics into curricula as shown in Fig 1.

A. Curriculum Development

Clear learning objectives that can be set for effectively teaching about the Dark Web include understanding its structure, recognizing associated risks and threats, and grasping the legal and ethical implications of navigating the Dark Web. Such learning can be enhanced by developing focused content modules to be included in the already existing cybersecurity courses, covering topics such as Dark Web architecture, types of illegal activities that are most current and popular, tools used—like Tor and I2P—and law enforcement methods to counter these activities. Adding real-world case studies illustrates these insights: how the Dark Web is leveraged in cybercrime, how data from it supports cyber investigations, and the ethical challenges that face cybersecurity experts working in such fields. Teaching people about the Dark Web requires a strong emphasis on ethical responsibility, discussing the moral implications and potential consequences of interactions involving this arena.

B. Teaching Methods

Dark Web education can be enhanced by incorporating interactive lectures, which combine theoretical instruction with discussions to stimulate critical thinking on the ethical and legal challenges surrounding the Dark Web. Hands-on labs provide students with practical experience in a controlled environment, allowing them to safely explore aspects of the Dark Web, such as accessing ".onion" sites through Tor, while ensuring that all activities adhere to legal and ethical standards. Additionally, guest speakers from law enforcement, cybersecurity, or ethical hacking bring real-world perspectives, enriching students' understanding with firsthand experiences [16], [17]. Group projects can further deepen this learning by encouraging students to research Dark Web topics, analyze trends in illegal marketplaces, or develop strategies for monitoring and mitigating Dark Web threats.

C. Assessment Strategies

To evaluate students' understanding of Dark Web concepts, quizzes and exams can include targeted questions on related topics. Research papers provide an opportunity for deeper investigation, encouraging students to engage in critical analysis of specific Dark Web issues. Student presentations foster knowledge sharing by allowing individuals to explore and present various aspects of the Dark Web to their peers. Practical assessments, including lab exercises and simulations, offer a hands-on approach to evaluating students' abilities to navigate, research, and analyze Dark Web content in a safe and ethical manner.

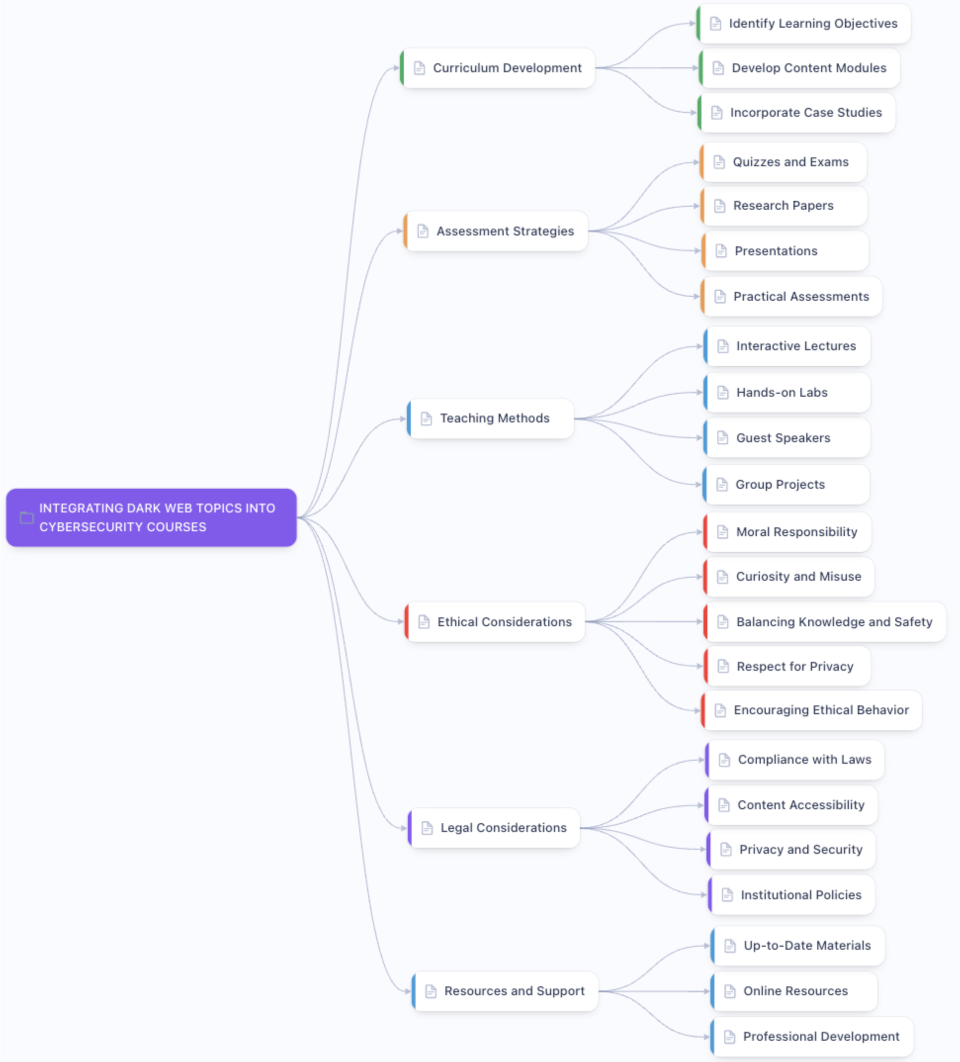

Fig. 1. ”Integrating Dark Web Topics into Cybersecurity Courses,” outlining key components for curriculum development. The map is organized into six primary categories: Curriculum Development, Assessment Strategies, Teaching Methods, Ethical Considerations, Legal Considerations, and Resources and Support. Each category includes specific elements such as identifying learning objectives, conducting practical assessments, emphasizing ethical behavior, ensuring compliance with laws, and providing professional development resources, offering a comprehensive framework for incorporating dark web topics into cybersecurity education.

D. Legal Considerations

Educators must ensure that all Dark Web-related activities and materials fully comply with applicable laws and avoid promoting any illegal actions. Content should focus on theoretical knowledge, steering clear of any illegal Dark Web material. Privacy and security are critical components, with instruction emphasizing protective measures to safeguard identity and personal information. Additionally, course content and teaching methods should align with institutional policies on Internet use and cybersecurity, ensuring consistency with the educational institution’s standards and guidelines.

E. Ethical Considerations

Managing student curiosity while simultaneously preventing misuse by addressing risks and legal implications associated with investigating the Dark Web is very important. Educators must reach equilibrium in teaching knowledge while safeguarding students to protect them from potentially detrimental information. Only by updating course materials and resources regularly will the Dark Web be taught well, considering the fast pace at which the topics change. Utilizing online resources, including platforms, forums, and databases, provides valuable information and insights into Dark Web topics.

F. Resources and Support

In addition, it is important that there are opportunities for faculty professional development, such as workshops, webinars, and conferences, to keep up with recent progress in Dark Web research and cybersecurity methodologies. This will ensure that both educators and students stay abreast of the prevailing trends and obstacles in this fast-evolving domain. By being able to include Dark Web topics in cybersecurity courses, educators could give students a broader view of the cyber threat landscape, including the challenges and ethical issues of navigating and confronting activities on the Dark Web.

V. Developing Learning Objectives and Outcomes Related to the Dark Web

In developing any cybersecurity curriculum module on the Dark Web, technical knowledge should be balanced with legal and ethical considerations. The following structured learning objectives and expected outcomes serve as a general guideline to develop education materials in this domain.

The learning objectives of this module are to understand the structure and nature of the Dark Web, to appreciate its legal and ethical implications, to identify the associated cybersecurity threats and to develop skills to navigate this part of the web in a safe and legal manner. Students shall learn differentiating between the Surface Web, Deep Web, and Dark Web and get familiar with such tools as Tor, I2P, and Freenet. Other aspects that this course will cover are the explanation of the legal frameworks and concerns for ethics about Dark Web activities; this will be able to keep them assessing whether what interactions are considered legal or illegal, as well as explore the challenges of accessing this online space.

On completion of the module, students will be able to apply safe and responsible navigation techniques, learn how to apply cyber-security good practices when accessing Dark Web resources, and understand the place of the Dark Web in cyber investigations with a view to appreciating how the police and cybersecurity professionals use it to gather intelligence. This will also involve an introduction to basic cyber forensic techniques that apply to Dark Web data collection.

The learning outcomes of the module do indeed enable students to use their knowledge responsibly: to describe the structure and purposes of the Dark Web, to identify what activities are legal or illegal, and to browse it safely by using security measures. These analytical skills will develop an understanding of the risk and threats that the Dark Web has at the organizational level, and students will be asked to proffer strategies that could integrate Dark Web intelligence within cybersecurity practices effectively. They would also critically review the existing laws and regulations dealing with the activities of the Dark Web, apply ethics-based reasoning to decide about the usage of the Dark Web intelligence in cybersecurity scenarios.

VI. A Structured Outline of a Module on Dark Web

A Dark Web module, in an educational resource like a textbook or lecture series, must be all-inclusive in terms of all aspects so that readers or students gain full insight. An outline for such a module, with a focus on the need to teach and include in cybersecurity curricula, is hereby proposed as shown in Fig 2.

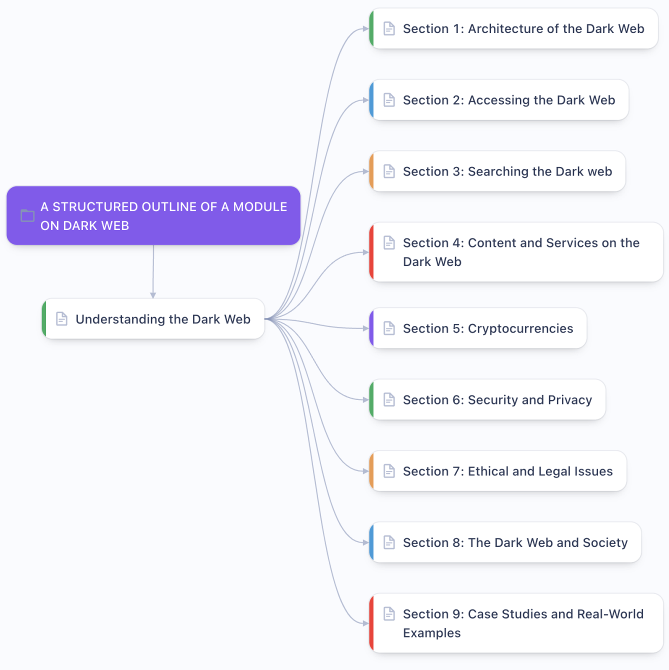
A STRUCTURED OUTLINE OF A MODULE ON DARK WEB
Understanding the Dark Web
Section 1: Architecture of the Dark Web
Section 2: Accessing the Dark Web
Section 3: Searching the Dark web
Section 4: Content and Services on the Dark Web
Section 5: Cryptocurrencies
Section 6: Security and Privacy
Section 7: Ethical and Legal Issues
Section 8: The Dark Web and Society
Section 9: Case Studies and Real-World Examples

Fig. 2. A structured outline of a module on the Dark Web, detailing sections on topics such as architecture, access, content, security, legal issues, and real-world case studies. This visual provides a comprehensive roadmap for understanding various aspects of the Dark Web within an educational framework.

Proposed chapter title: Understanding the Dark Web The chapter first starts with a basic definition of the Dark Web, including a short history and how it has been developed over time. Its further dwells are on the differences between the Dark Web, Deep Web, and Surface Web to set a base for the placement of the Dark Web within the greater perspective in the Internet world. These elements together have created a foundation for further investigation of the technical, ethical, and security implications associated with the Dark Web.

Section 1: Architecture of the Dark Web: This section provides the background of how the Dark Web works, from the very beginning when technologies such as Tor, I2P, and Freenet allowed it to happen, along with the anonymity and encryption mechanisms that kept it well hidden from general view. It covers the structure of the Dark Web and the various types of services it hosts, providing a thorough look at how users can access and navigate this concealed part of the Internet.

Section 2: Accessing the Dark Web: For accessing the Tor network, a few pieces of technology are involved in this section; most notably, the Tor Browser and access through VPNs. Instructions will be provided for safe access. Explanations about what the VPN provides in conjunction with the Tor network, risks, and reasons to take certain precautions in safely navigating the Dark Web are presented. There is also a discussion on ethical and legal considerations with the purpose of helping the user understand responsibilities and possible ramifications associated with access to the Dark Web.

Section 3: Searching the Dark Web: This section describes the methods of discovering services on the Darknet with the help of special Darknet search engines and the lists of Onion services. Guidelines on how to find those services and navigate through them, starting from the most common search engines created for search within the Onion network.

Section 4: Content and Services on the Dark Web: The subject areas to be covered in this chapter include an overview of the Dark Web, followed by distinguishing the different types of legal and illegal activities hosted on the network. This will include marketplaces, forums, services, and other websites with case studies, such as Silk Road, that detail its impact on current affairs. It goes on to discuss the Dark Web and the impact it has on privacy and free speech, bringing out both the pros and risks it causes to its users.

Section 5: Cryptocurrencies: This chapter introduces cryptocurrencies; it outlines what they are and how they operate, and it views their importance on the Dark Web. It then digs into the reasons why cryptocurrencies such as Bitcoin and Monero are popularly adopted to perform transactions, considering their privacy features. Furthermore, it directs how one should set up secure wallets for Bitcoin and Monero toward safe and anonymous transactions in the dark web.

Section 6: Security and Privacy: The section will discuss malware, scams, and various other illegal threats existing on the Dark Web. This section further discusses how the Dark Web, in turn, has been a facilitator of data breach disclosures and cyber espionage, thereby underlining the personal security measures that users themselves must take in order for them to stay safe. It goes on to address the challenges in tracking illicit activities by law enforcement and talks of broader cybersecurity implications and responses to tackle the evolving threats [18].

Section 7: Ethical and Legal Issues: This section explores the moral issues present in accessing the use of the Dark Web, and further surveys the complicated legal environment which controls its use. The section then sets real context to these challenges through real case studies of high-profile legal fights and law enforcement operations. The section opens up one avenue of discussion in the sensitive balancing act between privacy, anonymity, and legality that is increasingly debated with respect to Dark Web usage.

Section 8: The Dark Web and Society: This section looks into the function and role of the Dark Web in current society, based on its positive and negative uses. The Dark Web allows for journalism, activism, and the protection of privacy for those in regions that are oppressive. On the other end of the spectrum, criminal activities and illicit markets exist concerning the Dark Web. This section concludes with the future outlook of the Dark Web in consideration of societal implications and the impact of shifting times that affect privacy, security, and ethical considerations.

Section 9: Case Studies and Real-World Examples: This section offers a detailed examination of significant incidents involving the Dark Web, analyzing major law enforcement operations and cybersecurity breaches tied to its use. Additionally, it presents stories where anonymity and privacy on the Dark Web have had positive impacts, showcasing the platform's complex role in supporting both security challenges and beneficial causes.

VII. HANDS-ON ACTIVITIES ON DARK WEB AND DARKNET

A. Guidelines for educators

Incorporating hands-on activities and simulations related to the Dark Web into cybersecurity courses requires careful consideration of legal, ethical, and security issues. It is vital that educators first establish explicit learning objectives and consider how these kinds of activities will serve to further broader goals, such as developing an understanding of cybersecurity threats and measures to defend against them, without in any way promoting or encouraging illegal or unethical behavior. The emphasis that needs to be drilled from the beginning of every activity is on legal and ethical standards, essentially through educators discussing the repercussions of crossing boundaries both in a legal and professional sense and making students understand where the line between legality and illegality stands regarding Dark Web activities.

The use of simulated environments is considered a harmless way to learn about the Dark Web without some of the involved risks. The classroom environment should be controlled by the educators through such means as network isolation, making use of virtual machines or secure networks which block any form of unauthorized access. In addition, instructions are given in terms of specific guidelines on what one can and cannot do in step-by-step terms, allowing only prescribed doings and forbidding any actions concerning illegal content or unauthorized interaction in the Dark Web.

Focusing on defensive techniques, such as identifying phishing attempts and recognizing leaked data, steers activities toward prevention and response, rather than offensive actions. Educators can use de-identified or synthetic data to demonstrate how personal data is traded on the Dark Web without compromising privacy. Critical thinking and discussion should follow each activity, encouraging students to reflect on the ethical implications, risks, and professional applications of the knowledge they gain.

By following these guidelines, educators can create a safe, legal, and ethical learning framework for students to explore the Dark Web and its cybersecurity implications. This approach allows students to gain valuable skills and insights without exposing them to unnecessary risks.

B. Hands-on lab creation phases

Creating a hands-on lab to teach students how to access and use the Dark Web requires careful planning to maintain ethical, legal, and secure standards. The lab must operate within a controlled, secure, and compliant environment, with educators pre-screening content to ensure adherence to all applicable laws and institutional policies. This structured approach is divided into major phases to ensure a successful hands-on experience. This also involves the discussion and reflection phase of ethical and legal ramifications implicit in the use of the Dark Web.

To this end, through the application of such stages, instructors will be able to offer a comprehensive hands-on lab in a manner that students learn about the Dark Web in an appropriate, safe, legal, and ethical manner. In other words, practical understanding can be developed at the same time while assuring responsible behavior.

By following these phases, educators can create a comprehensive hands-on lab that educates students about the Dark Web in a secure, legal, and ethical manner, fostering practical understanding while prioritizing responsible behavior.

VIII. AI-Based Hands-on Labs on Dark Web and Darknet Traffic

This can be achieved by integrating Artificial Intelligence into the hands-on lab in cybersecurity education and training as a pedagogical methodology towards leading-edge techniques. One will get better performance in equipping students and professionals to meet modern cyber challenges with novel and effective solutions. It will help in strengthening technical skills, as well as in acquiring critical thinking and adaptive problem-solving abilities, crucial in the ever-changing world of cybersecurity. It provides realism with efficiency and interactivity to the learning experience when AI is integrated into cybersecurity labs. Such sophisticated AI-enabled simulations cannot be done manually but can give students a highly realistic and hands-on experience with the real threat scenario. Efficiency is increased through automation of repetitive tasks, hence allowing students to invest more time in high-order problem solving and thinking at the strategic level. While the methods of cyber-attacks are becoming sophisticated, AI-driven, lab training helps the students prepare for modern threats by equipping them to manage offensive and defensive AI applications. In addition to this, adaptive AI tools facilitate interactive learning and thereby make the training sessions more interesting and fruitful.

Moreover, hands-on labs on Dark web and Darknet are usually conducted using mainly two phases. In the first phase, students require to select the appropriate datasets for the analysis and classification of Dark web content and Darknet traffic [19], [20]. In the second phase, the students are asked to implement machine learning models for Dark web content and Darknet traffic classification. Additional hands-on labs that simulate Darknet networks can provide students with practical experience in modeling and analyzing traffic within Darknet environments, particularly focusing on Tor networks as given in Fig 3.

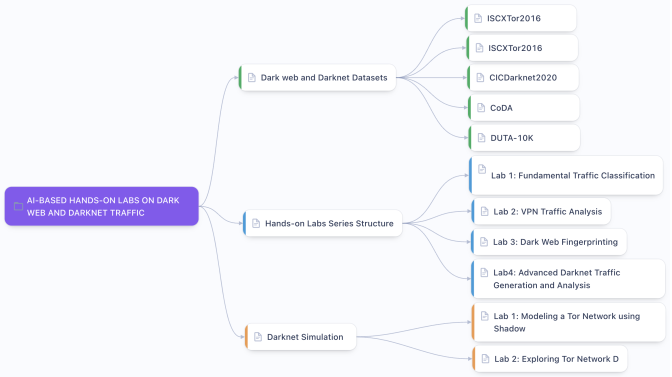
AI-BASED HANDS-ON LABS ON DARK WEB AND DARKNET TRAFFIC
Dark web and Darknet Datasets
ISCXTor2016
ISCXTor2016
CICDarknet2020
CoDA
DUTA-10K
Hands-on Labs Series Structure
Lab 1: Fundamental Traffic Classification
Lab 2: VPN Traffic Analysis
Lab 3: Dark Web Fingerprinting
Lab4: Advanced Darknet Traffic Generation and Analysis
Darknet Simulation
Lab 1: Modeling a Tor Network using Shadow
Lab 2: Exploring Tor Network D

Fig. 3. Overview of AI-based hands-on labs on Dark Web and Darknet traffic, covering datasets and lab series structure. The modules include analysis of datasets , traffic classification, VPN and Dark Web analysis, and darknet simulation labs, offering practical learning on Darknet environments and traffic patterns.

A. Dark web and Darknet Datasets Overview

This section presents an overview of the datasets used in the analysis and classification of Dark web contents and Darknet traffic, focusing on their types and the unique characteristics of each. Understanding these datasets is crucial for developing effective machine learning models that can differentiate between various traffic types and identify suspicious activities within the Darknet ecosystem. The following is a list of well-known datasets for conducting Dark web content and Darknet traffic classification and analysis Table II:

TABLE II
Overview of Datasets Related to Dark Web and Tor Traffic

Dataset Name	Type of Traffic	Description
ISCXTor2016	Tor and non-Tor traffic	Contains approximately 2.5 million labeled flows, captured over two weeks, including normal traffic [21], [22].
ISCXVPN2016	VPN and non-VPN traffic	Captures 14 categories of traffic (regular, VPN-encrypted) including activities like VoIP, P2P, file transfer, and web browsing through apps like Skype, Facebook, and uTorrent [23].
CICDarknet2020	VPN, non-VPN, Tor, and non-Tor traffic	Employs a two-layer architecture to capture and categorize traffic. Includes identified flows and dark traffic from various categories.
CoDA	Dark Web documents	Comprehensive Darkweb Annotations (CoDA) corpus with 10,000 Dark Web documents. English is the most frequent language, followed by Russian, German, and French.
DUTA-10K	Dark Web hidden services	Contains 10,367 labeled onion addresses; 20% classified as suspicious and 48% as normal content [15].

B. Hands-on Labs Series Structure

The following series of practical labs will introduce the students to hands-on analysis and classification of Dark web contents and Darknet traffic. Each lab examines the different aspects of network analysis and traffic classification.

Fundamental Traffic Classification: This lab is dedicated to binary classification for Tor vs. non-Tor traffic. The working dataset will be ISCXTor2016. Students will implement the following machine learning models based on GBoost, DT, RF, LR, and SVM. The lab will start with feature extraction from network flows, moving toward the analysis of temporal patterns. As most of the samples are imbalanced, the assessment section should rely on the precision-recall metric and ROC curves.

VPN Traffic Analysis: Using the ISCXVPN2016 dataset, students will classify traffic in such a way that separate regular and VPN-encapsulated versions of services can be differentiated. Among these would fall feature engineering-flow entropy and temporal sequence modeling that enable deep learning models like LSTMs and attention mechanisms to identify very slight differences in encrypted traffic patterns. Students are going to analyze behavior variations of applications while developing service fingerprinting metrics over VPN.

Dark Web Fingerprinting: This lab will employ structural classification for Dark Web content provided by the CoDA and DUTA-10K datasets. Students are expected to build a classification by combining text analysis techniques with state-of-the-art language models, including but not restricted to BERT, RoBERTa, DistilBERT, ALBERT and XLM-RoBERTa. By using natural language, students will identify Dark Web linguistic patterns, perform ranking to rank hidden services, and develop classifiers that will detect suspicious domain clones.

Advanced Darknet Traffic Generation and Analysis: This lab will review the creation of an integrated Darknet traffic analytics platform. They would employ GANs in the generation of synthetic Darknet traffic in order to enhance classifier robustness. Also, explore various defensive techniques such as Traffic Padding and Flow Transformation to defeat the traffic analysis.

C. Darknet Simulation

The Darknet simulation assigns practical experience to students in modeling and analyzing traffic within Darknet environments, including those involving Tor networks. This realistic platform allows the students to delve deep inside various issues regarding anonymous communications and challenges associated with maintaining privacy and security in such networks.

Modeling a Tor Network using Shadow: This lab is aimed at introducing students to the Shadow network simulator through modeling a Tor network for observing exactly how Tor provides mechanisms for anonymous communication. Shadow executes real Tor software in an emulated environment by intercepting system calls, which allows it to really emulate network behavior. This lets students analyze performance and attack resilience in a controlled Tor-like environment.

Exploring Tor Network Dynamics: Using the metrics.torproject.org, students, while working in this lab with data, will gain information about the users, servers, traffic, performance, onion services, and applications of the Tor network. Also, interactively query information about relays or bridges in the public Tor network using services. They would also help students investigate the diversity of the networks in order to appreciate some of the operational difficulties and security features of Tor. These are all supposed to give an overview as to how Tor maintains its anonymity and works appropriately against any kind of vulnerability.

ASSESSING STUDENTS

A. Quiz Design on Dark Web Topics

Creating quizzes helps reinforce students' understanding of the Dark Web. Quizzes should range from basic to advanced, covering various aspects, including technology, legality, and usage contexts.

B. Examples of Quiz Questions on the Dark Web

1) Basic Level:

- True or False: The Dark Web is entirely illegal to access.
- Multiple Choice: Which tool is commonly used to access the Dark Web? (A) Google Chrome (B) Tor Browser (C) Internet Explorer (D) Safari
- Fill in the Blank: The part of the Internet that is not indexed by traditional search engines is called the _____.
- Matching: Match terms with definitions:
  - Dark Web - Part of the Internet requiring specific tools and not indexed by search engines.
  - Deep Web - Not indexed by search engines but accessible with standard web browsers.
  - Surface Web - Indexed by search engines.

2) Intermediate Level:

- Multiple Choice: Which activity is legal on the Dark Web? (A) Buying stolen credit card info (B) Accessing government documents without permission (C) Using anonymous services for privacy (D) Selling illegal drugs
- True or False: All information on the Dark Web is used for criminal purposes.
- Fill in the Blank: The _____ protocol ensures anonymity on the Dark Web.
- Short Answer: Discuss ethical considerations when researching the Dark Web.

3) Advanced Level:

- Multiple Choice: Which is a challenge for law enforcement on the Dark Web? (A) Lack of anonymity (B) Overabundance of clear-text data (C) Encryption and use of cryptocurrencies (D) Easy traceability of users
- True or False: It's impossible to collect Dark Web data for academic purposes without breaking the law.
- Short Answer: Describe how the Tor network maintains user anonymity.
- Essay: Discuss the implications of the Dark Web on national security and individual privacy.

C. Practical Application

As a cybersecurity professional monitoring Dark Web threats, it's essential to follow ethical guidelines that balance respect for privacy with public safety. If you encounter a site selling stolen data, document steps aligning with legal protocols, report to authorities, and avoid illegal transactions. Responsible actions ensure effective threat management and uphold professional ethics.

D. Examples of Quiz Questions on Cryptocurrencies

Questions should range from basic to advanced, covering cryptocurrency use on the Dark Web, including anonymity, legality, and transaction types.

1) Basic Level:

- True or False: Cryptocurrencies are used on the Dark Web exclusively for illegal transactions.
- Multiple Choice: What is the primary reason cryptocurrencies are used on the Dark Web? (A) High-speed transactions (B) Anonymity (C) Investment (D) Avoiding bank fees.

2) Intermediate Level:

- True or False: Cryptocurrency transactions on the Dark Web are completely untraceable.
- How do cryptocurrencies maintain anonymity? (A) Centralized database (B) User location (C) Private and public keys (D) Personal information registration.

3) Advanced Level:

- What method enhances anonymity in cryptocurrency transactions on the Dark Web? (A) Multiple bank accounts (B) Mixing services (C) Large transactions only (D) Public Wi-Fi usage.
- How do law enforcement agencies combat illegal cryptocurrency transactions? (A) Banning transactions (B) Tracking blockchain (C) Creating their own cryptocurrencies (D) Shutting down the internet.

IX. Conclusion

Researching and understanding the Dark web is a critical and essential step in fighting and preventing cybercrime. However, studying the Dark web poses unique challenges. This educational paper explored the significance of incorporating Dark Web education into cybersecurity curricula to better prepare the next generation of cybersecurity professionals. This study assessed current educational practices and identified gaps in knowledge regarding the Dark Web among cybersecurity students, and the complete absence or the limited contents on Dark Web topics offered in most cybersecurity curricula around the world. Findings suggest that a comprehensive understanding of the Dark Web can significantly contribute to enhance students' ability to identify, analyze, and mitigate cyber threats. As a consequence, the paper proposed a framework for successfully integrating Dark Web topics into cybersecurity courses, highlighting legal and ethical considerations and the balance between awareness and practical skills. This work underscores the importance of evolving cybersecurity education to address emerging cyber threats effectively.

References

[1] J. J. V. Pergolizzi, J. A. Ba, J. R. Taylor, and R. B. R. N. R. Group, "The 'darknet': The new street for street drugs," *Journal of Clinical Pharmacy and Therapeutics*, vol. 42, no. 6, pp. 790–792, 2017.

[2] F. T. Ngo, C. Marcum, and S. Belshaw, "The dark web: What is it, how to access it, and why we need to study it," *Journal of Contemporary Criminal Justice*, vol. 39, no. 2, pp. 160–166, 2023.

[3] S. H. Belshaw, B. Nodeland, L. Underwood, and A. Colaiuta, "Teaching about the dark web in criminal justice or related programs at the community college and university levels," *Journal of Cybersecurity Education, Research and Practice*, vol. 2019, no. 2, 2020.

[4] Z. Trabelsi and W. Ibrahim, "Teaching ethical hacking in information security curriculum: A case study," in *2013 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 2013, pp. 130–137.

[5] S. Sobhan *et al.*, "A review of dark web: Trends and future directions," in *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, Los Alamitos, CA, USA, 2022, pp. 1780–1785.

[6] G. Janchenko, K. Paullet, and F. Hartle, "Introducing the deep and dark web into higher education pedagogy: An exploratory study," *Issues in Information Systems*, vol. 21, no. 1, pp. 141–146, 2020.

[7] George Mason University, "Dfors 780 syllabus: Exploring the darknet," Syllabus, 2021, available online: https://dfor.gmu.edu/wp-content/uploads/2021/09/DFORS-780_Exploring-the-Darknet_F21_-VARGAS.pdf.

[8] ——, "Dfor 780 syllabus: Darknet technologies," Syllabus, 2022, available online: https://dfor.gmu.edu/wp-content/uploads/2022/08/2022-FALL-DFOR-780-SYLLABUS-VARGAS.pdf.

[9] Ferris State University, "Isi program to develop grant-funded social media/dark web analysis curriculum, cyber competitions," News Article, 2019, available online: https://www.ferris.edu/news/archive/2019/january/grant.htm.

[10] Georgia State University, "Darknet intelligence certificate program," Program Outline, 2024, available online: https://ebcs.gsu.edu/TRAININGS/DARKNET-INTELLIGENCE-CERTIFICATE-PROGRAM/.

[11] Charles Sturt University, "Itc578 dark web," Subject Outline, 2022, available online: https://www.csu.edu.au/handbook/handbook19/subjects/ITC578.html.

[12] Cyberlaw University, "Mystery of darknet law," Course Outline, 2023, available online: https://cyberlawuniversity.com/online-cyber-law-courses-online/mystery-of-Darknet-law/.

[13] Z. Trabelsi and M. McCoey, "Ethical hacking in information security curricula," *International Journal of Information and Communication Technology Education (IJICTE)*, vol. 12, no. 1, pp. 1–10, 2016.

[14] F. Saidi, Z. Trabelsi, K. Salah, and H. B. Ghezala, "Approaches to analyze cyber terrorist communities: Survey and challenges," *Computers & Security*, vol. 66, pp. 66–80, 2017.

[15] M. W. Al-Nabki, E. Fidalgo, E. Alegre, and L. Fernández-Robles, "Torank: Identifying the most influential suspicious domains in the tor network," *Expert Systems with Applications*, vol. 123, pp. 212–226, Jun. 2019.

[16] S. Retzkin, *Hands-On Dark Web Analysis: Learn what goes on in the Dark Web, and how to work with it*. Dec. 26: Packt Publishing, 2018.

[17] Z. Trabelsi and W. El-Hajj, "On investigating arp spoofing security solutions," *International Journal of Internet Protocol Technology*, vol. 5, no. 1-2, pp. 92–100, 2010.

[18] Z. Trabelsi, H. El-Sayed, L. Frikha, and T. Rabie, "Traceroute based ip channel for sending hidden short messages," in *Advances in Information and Computer Security: First International Workshop on Security, IWSEC 2006, Kyoto, Japan, October 23-24, 2006. Proceedings 1*. Springer, 2006, pp. 421–436.

[19] G.-Y. Shin *et al.*, "Dark side of the web: Dark web classification based on textcnn and topic modeling weight," *IEEE Access*, vol. 12, pp. 36 361–36 371, 2024.

[20] Z. Trabelsi, T. Qayyum, K. Hayawi, and M. Ali, "Global aggregation node selection scheme in federated learning for vehicular ad hoc networks (vanets)," in *2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*, 2022, pp. 1–6.

[21] S. Al-E'mari, Y. Sanjalawe, and S. Fraihat, "Detection of obfuscated tor traffic based on bidirectional generative adversarial networks and vision transform," *Computers & Security*, vol. 135, p. 103512, 2023.

[22] C. Johnson, B. Khadka, E. Ruiz, J. Halladay, T. Doleck, and R. B. Basnet, "Application of deep learning on the characterization of tor traffic using time-based features," *Journal of Internet Services and Information Security*, vol. 11, pp. 44–63, Jan. 2021.

[23] Y. Zhou, H. Shi, Y. Zhao, W. Gao, and W. Zhang, "Encrypted network traffic identification based on 2d-cnn model," in *2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Tainan, Taiwan, 2021, pp. 238–241.