

# FORENSISOFT: EARLY DETECTION OF ONGOING CYBER-ATTACKS

Mr. Mohammed Rahmat Ali<sup>1</sup>, Mohammed Maaz Ahmed<sup>2</sup>, Mohammed Ameen Hussain<sup>3</sup>, Syed Zeeshan Ullah Ghouri<sup>4</sup>

<sup>1</sup>Assistant Professor, Department of CSE, ISL College of Engineering, Hyderabad, India.

<sup>2,3,4</sup>B. E Student, Department of CSE, ISL College of Engineering, India.

**Abstract:** Traditional attack detection approaches utilize predefined databases of known signatures about already-seen tools and malicious activities observed in past cyber-attacks to detect future attacks. More sophisticated approaches apply machine learning to detect abnormal behavior. Nevertheless, a growing number of successful attacks and the increasing ingenuity of attackers prove that these approaches are insufficient. This paper introduces an approach for digital forensics-based early detection of ongoing cyber-attacks called Forensisoft. The approach combines ontological reasoning with the MITRE ATT&CK framework, the Cyber Kill Chain model, and the digital artifacts acquired continuously from the monitored computer system. Forensisoft examines the collected digital artifacts by applying rule based reasoning on the Forensisoft cyber-attack detection ontology to identify traces of adversarial techniques. The identified techniques are correlated to tactics, which are then mapped to corresponding phases of the Cyber Kill Chain model, resulting in the detection of an ongoing cyber-attack. Finally, the proposed approach is demonstrated through an email phishing attack scenario.

## INTRODUCTION

Organizations must deal with cyberattacks to accomplish their objectives, not as a best practice. The Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) established the Cyber Security Framework, which includes detection as one of five cyber security tasks. Threat detection may occur before a cyber-attack, when attackers do reconnaissance and weaponization. It may happen during a cyber assault (early detection of ongoing cyber-attack) or afterward (post-compromise detection), when hackers achieve their goals.

Statistics-based, pattern-based, rule-based, state-based, and heuristic-based detection methods exist. Statistics-based techniques profile a monitored system and identify cyber-attacks as anomalous behaviors above an ordinal baseline. To identify cyberattacks, pattern-based techniques seek for predetermined data or behavior patterns. Rule-based techniques diagnose cyber attacks by running rules against a system. Rules are mainly if-then sentences that

simulate harmful behavior. Rule extensions and maintenance are easier than pattern extensions and maintenance since they do not predefine large patterns. State-based cyber-attack detection algorithms use finite state machines. Heuristic-based techniques employ a model, decision-making algorithm, and conditions and rules.

Current detection methods struggle to identify ongoing cyberattacks, hence more should be done. In 2020, enterprises discovered 59% of security events, and the typical stay duration of an adversary inside a compromised firm was 24 days, according to Mandiant's threat report. When third parties discover the assault instead of the organization, the dwell period might be significantly longer. MITRE also noted the shortcomings of present detection methods.

MITRE created the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework to aid rule-based detection. This framework describes how cyberattackers might accomplish short-term aims, termed tactics. Thus, an MITRE ATT&CK-based detection strategy should identify a system's strategies and tactics and use them to detect a cyber-attack as soon as feasible. As described in, most MITRE ATT&CK-based cyber-attack detection methods only identify technique operation. They just examine event logs and network traffic captures and do not use the plethora of digital artifacts created during system operation.

Since digital relics may comprise both volatile (processes and RAM contents) and non-volatile (event logs, emails) data, they can reveal more about user and system activities. Thus, an effective cyber-attack detection method should use digital artifacts more. To protect their integrity, digital forensics should be used to get them from the monitoring machine. The literature has noted the proactive use of digital forensics before or during cyberattacks. Forensisoft, a digital forensics method for early cyberattack detection, is suggested in this research. Forensisoft uses ontological reasoning, the MITRE ATT&CK framework, the Cyber Kill Chain (CKC) model, and digital artifacts from the monitored computer system using digital forensics. The MITRE ATT&CK architecture offers strategies for each cyber-attack phase, while the CKC model provides the sequence. Each approach leaves digital artifacts in the monitored computer system. The observed computer system's digital artifacts are examined by Forensisoft to discover operational methods. Then it maps

developed strategies into the CKC stages that rebuild a cyber-attack based on the CKC model to identify it. Identifying additional CKC model phases improves detection accuracy. The proposed Forensisoft implementation uses rule-based reasoning on the ontology. The Forensisoft ontology offers MITRE ATT&CK strategies, CKC stages, and digital forensics

properties in a machine-readable format. The suggested rule-based reasoning approach expresses Forensisoft detection logic declaratively and outputs CKC phases of ongoing cyberattacks. An email phishing assault illustrates the approach's usefulness.

### **PROPOSED SYSTEM :**

Digital forensics technique Forensisoft detects cyberattacks early. Digital forensics, ontological reasoning, the MITRE ATT&CK framework, the Cyber Kill Chain (CKC) concept, and monitored computer system artifacts are used by Forensisoft. The MITRE ATT&CK architecture provides cyber-attack phase methods, whereas the CKC model provides sequence. Each method leaves digital artifacts in the monitoring machine. Digital artifacts from the observed computer system are evaluated by Forensisoft to determine operating procedures. This is done by mapping the observed approaches into CKC stages and utilizing the CKC model to identify the cyberattack. Finding more CKC model phases increases detection. The suggested Forensisoft implementation leverages ontology-based rule-based reasoning. Forensisoft ontology turns MITRE ATT&CK tactics, CKC phases, and digital forensics features into machine-readable form. The rule-based reasoning technique declares Forensisoft detection logic and produces CKC stages of cyberattacks. A successful email phishing attack shows its value.

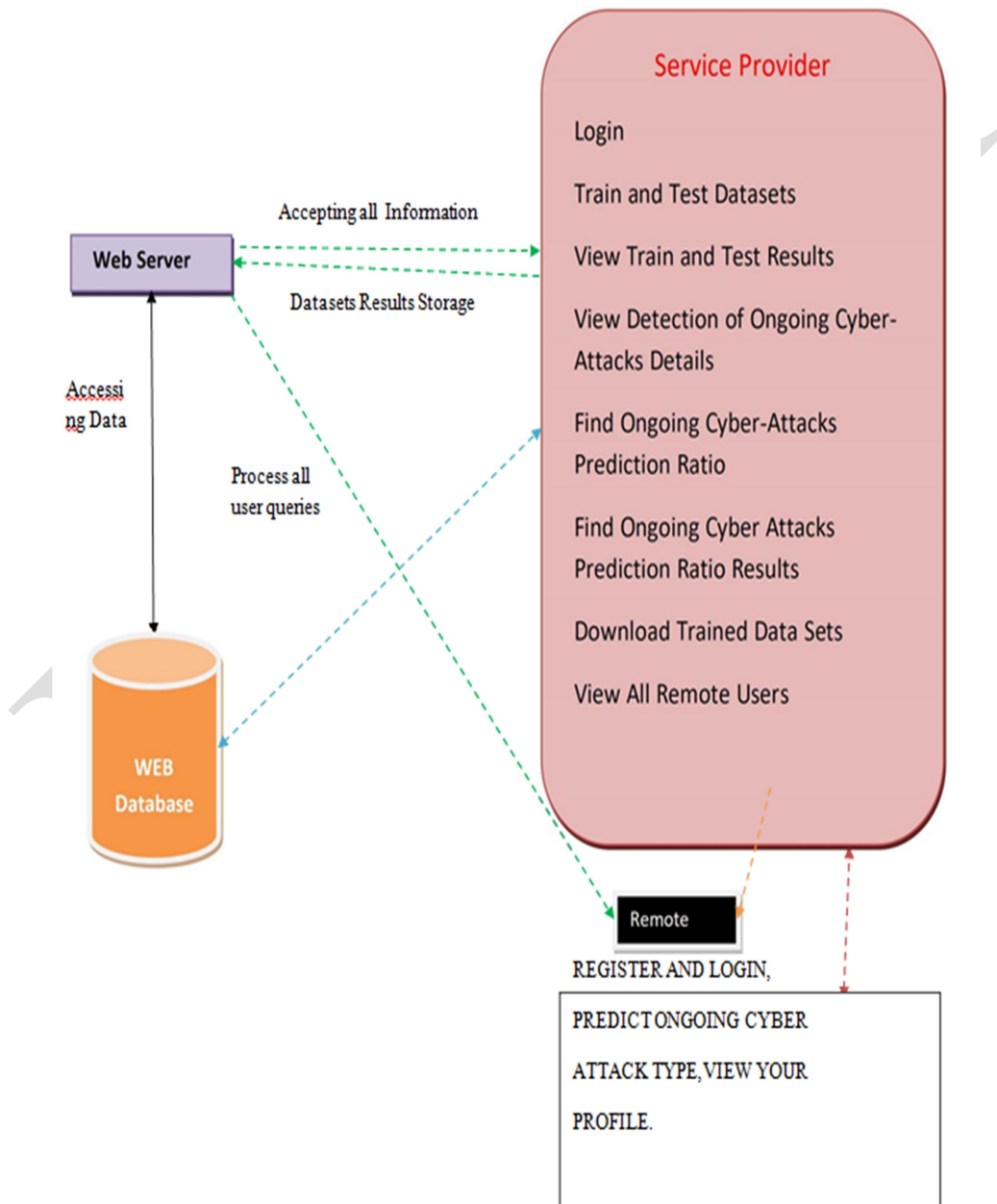
This research introduces cyberattack detection technology Forensisoft. Forensisoft's multi-step method utilizes CKC and MITRE ATT&CK. The multi-step technique reconstructs and identifies cyberattacks using monitored system digital artifacts.

### **LITERATURE SURVEY**

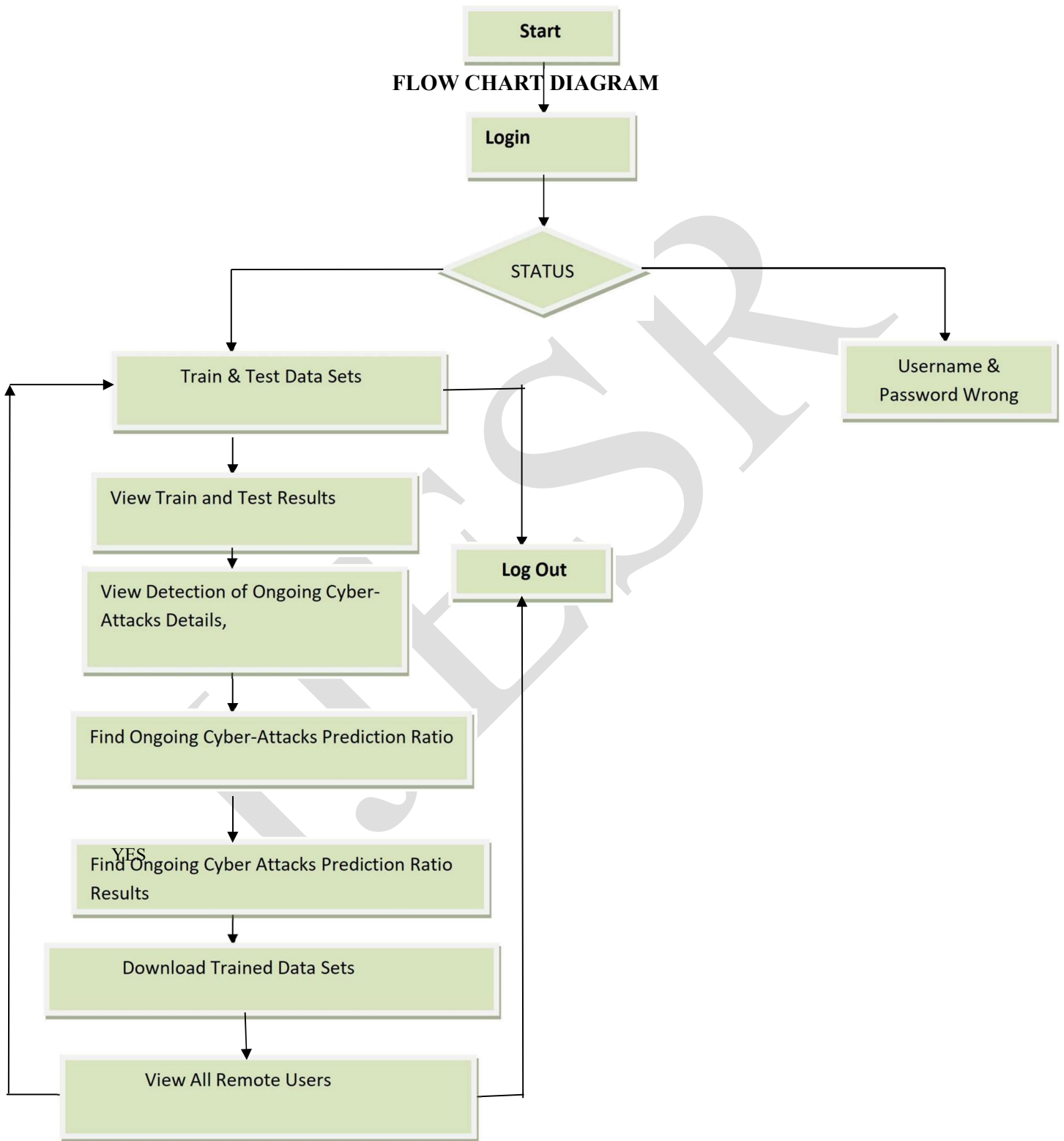
Conventional methods for detecting attacks rely on pre-established databases containing known signatures of tools and harmful behaviors that have been discovered in previous cyber-attacks. These databases are used to identify and detect future assaults. Advanced techniques use machine learning algorithms to identify anomalous activity. However, the rising number of successful assaults and the growing cleverness of attackers demonstrate that current methods are inadequate. This study presents a method called Forensisoft that uses digital forensics to identify cyber-attacks in their early stages. This technique integrates ontological reasoning with the MITRE ATT&CK framework, the Cyber Kill Chain concept, and the ongoing collection of digital artifacts from the monitored computer system. Forensisoft analyzes the gathered digital evidence by using rule-based logic on the

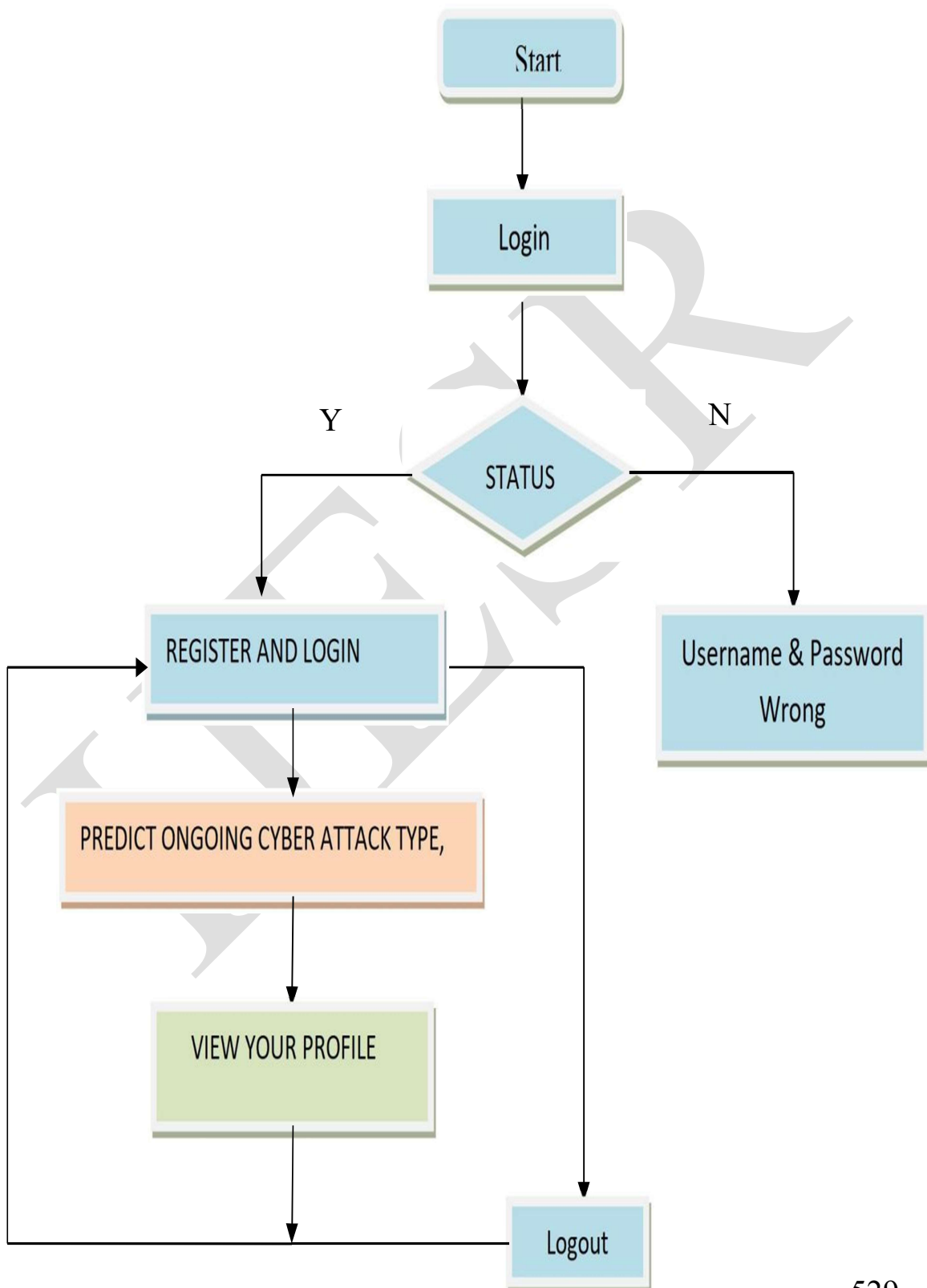
Forensisoft cyber-attack detection ontology to detect signs of adversarial methods. The detected approaches are associated with strategies, which are then linked to the respective stages of the Cyber Kill Chain model, ultimately leading to the identification of an ongoing cyber-attack. Ultimately, the suggested method is shown by means of an email phishing attack scenario.

### SYSTEM ARCHITECTURE DIAGRAM



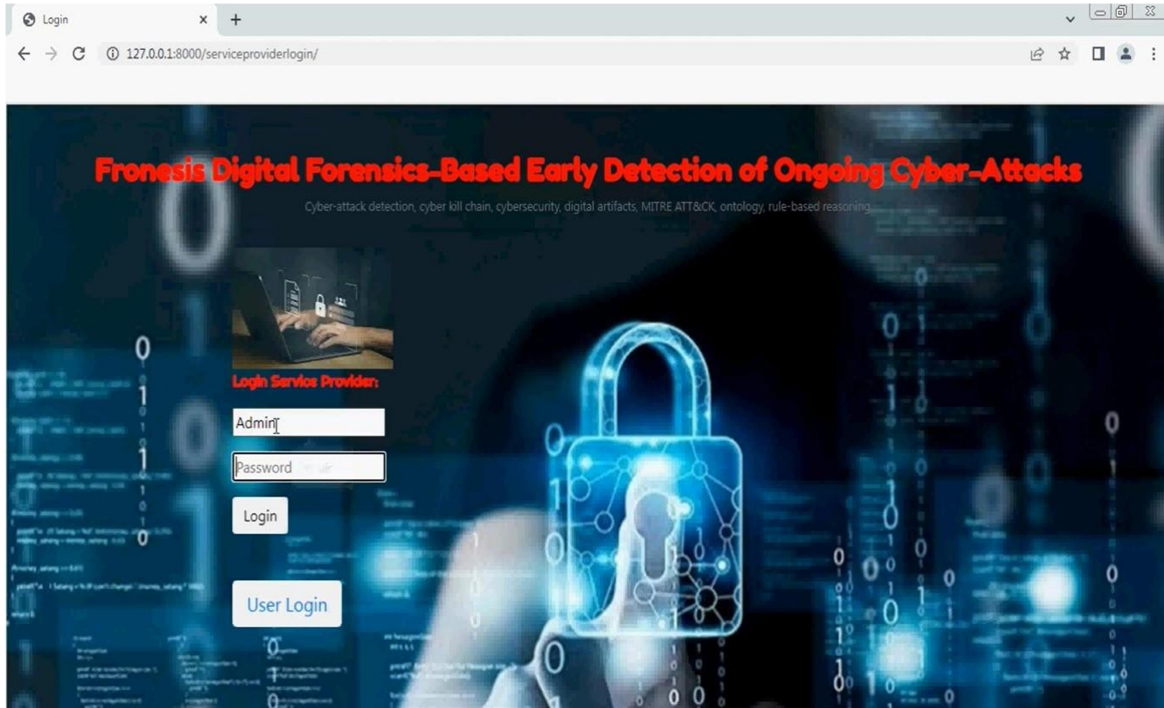
### FLOW CHART DIAGRAM



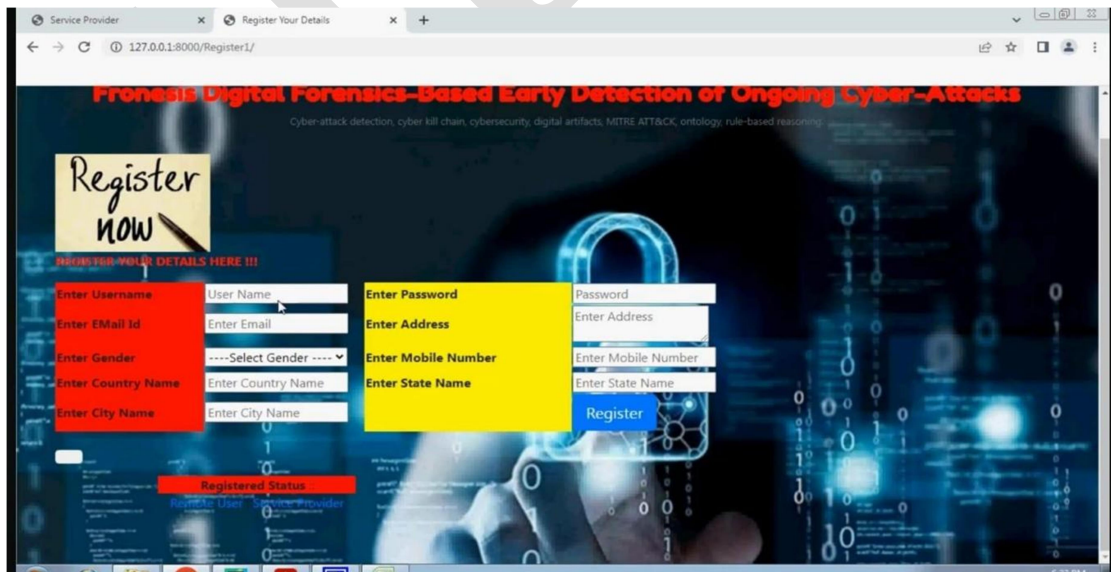




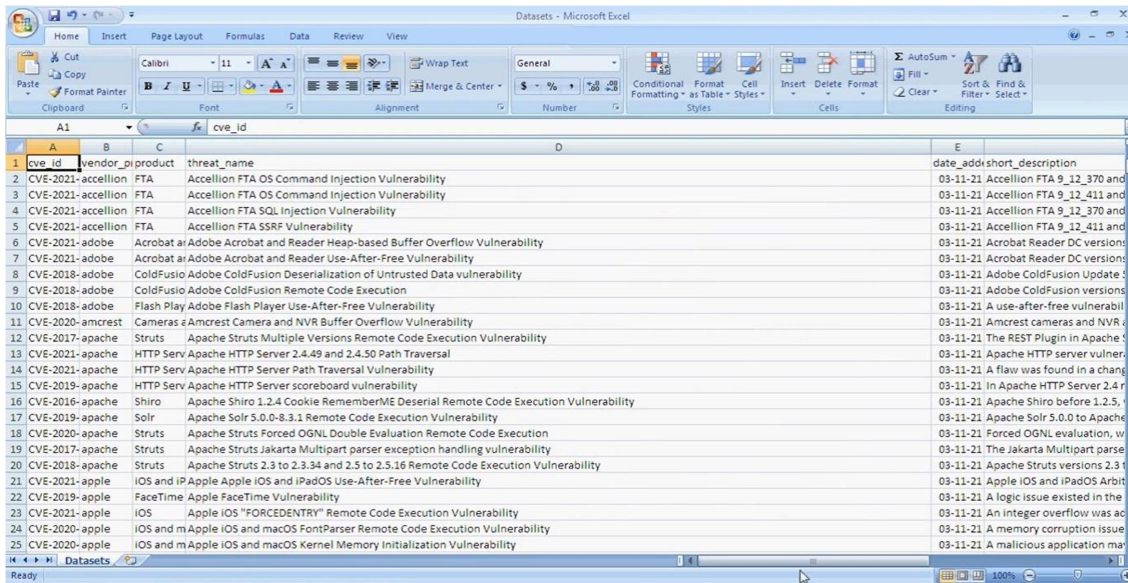
## RESULTS LOGIN PAGE



## USER REGISTRATION PAGE

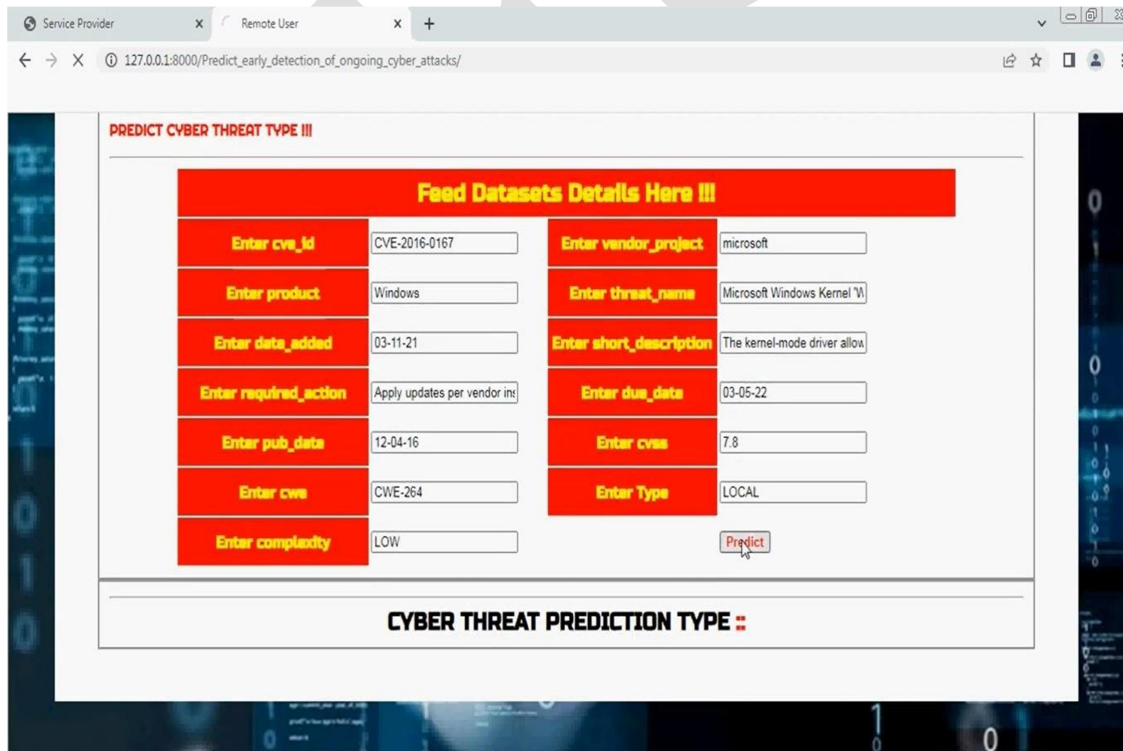


## DATASET



Cve_id	vendor_project	product	threat_name	date_added	short_description
CVE-2021-accellion	FTA	Accellion FTA OS Command Injection Vulnerability		03-11-21	Accellion FTA 9_12_370 and
CVE-2021-accellion	FTA	Accellion FTA OS Command Injection Vulnerability		03-11-21	Accellion FTA 9_12_411 and
CVE-2021-accellion	FTA	Accellion FTA SQL Injection Vulnerability		03-11-21	Accellion FTA 9_12_370 and
CVE-2021-accellion	FTA	Accellion FTA SSRF Vulnerability		03-11-21	Accellion FTA 9_12_411 and
CVE-2021-adobe		Acrobat and Adobe Acrobat and Reader Heap-based Buffer Overflow Vulnerability		03-11-21	Acrobat Reader DC versions
CVE-2021-adobe		Acrobat and Adobe Acrobat and Reader Use-After-Free Vulnerability		03-11-21	Acrobat Reader DC versions
CVE-2018-adobe		ColdFusion Adobe ColdFusion Deserialization of Untrusted Data vulnerability		03-11-21	Adobe ColdFusion Update 1
CVE-2018-adobe		ColdFusion Adobe ColdFusion Remote Code Execution		03-11-21	Adobe ColdFusion versions
CVE-2018-adobe		Flash Play Adobe Flash Player Use-After-Free Vulnerability		03-11-21	A use-after-free vulnerabil
CVE-2020-amcrest		Cameras and NVR Buffer Overflow Vulnerability		03-11-21	Amcrest cameras and NVR
CVE-2017-apache		Struts Apache Struts Multiple Versions Remote Code Execution Vulnerability		03-11-21	The REST Plugin in Apache
CVE-2021-apache		HTTP Serv Apache HTTP Server 2.4.49 and 2.4.50 Path Traversal		03-11-21	Apache HTTP server vulner
CVE-2021-apache		HTTP Serv Apache HTTP Server Path Traversal Vulnerability		03-11-21	A flaw was found in a chang
CVE-2019-apache		HTTP Serv Apache HTTP Server scoreboard vulnerability		03-11-21	In Apache HTTP Server 2.4.7
CVE-2016-apache		Shiro Apache Shiro 1.2.4 Cookie RememberME Deserial Remote Code Execution Vulnerability		03-11-21	Apache Shiro before 1.2.5,
CVE-2019-apache		Solr Apache Solr 5.0.0-8.3.1 Remote Code Execution Vulnerability		03-11-21	Apache Solr 5.0.0 to Apache
CVE-2020-apache		Struts Apache Struts Forced OGNL Double Evaluation Remote Code Execution		03-11-21	Forced OGNL evaluation, w
CVE-2017-apache		Struts Apache Struts Jakarta multipart parser exception handling vulnerability		03-11-21	The Jakarta multipart parse
CVE-2018-apache		Struts Apache Struts 2.3 to 2.3.34 and 2.5 to 2.5.16 Remote Code Execution Vulnerability		03-11-21	Apache Struts versions 2.3 t
CVE-2021-apple		iOS and iPadOS Apple iOS and iPadOS Use-After-Free Vulnerability		03-11-21	Apple iOS and iPadOS Arbit
CVE-2019-apple		FaceTime Apple FaceTime Vulnerability		03-11-21	A logic issue existed in the
CVE-2021-apple		iOS Apple iOS "FORCEENTRY" Remote Code Execution Vulnerability		03-11-21	An integer overflow was ac
CVE-2020-apple		iOS and macOS Apple iOS and macOS FontParser Remote Code Execution Vulnerability		03-11-21	A memory corruption issue
CVE-2020-apple		iOS and macOS Apple iOS and macOS Kernel Memory Initialization Vulnerability		03-11-21	A malicious application ma

## PREDICTING CYBER THREAT TYPE



**PREDICT CYBER THREAT TYPE III**

**Feed Datasets Details Here III**

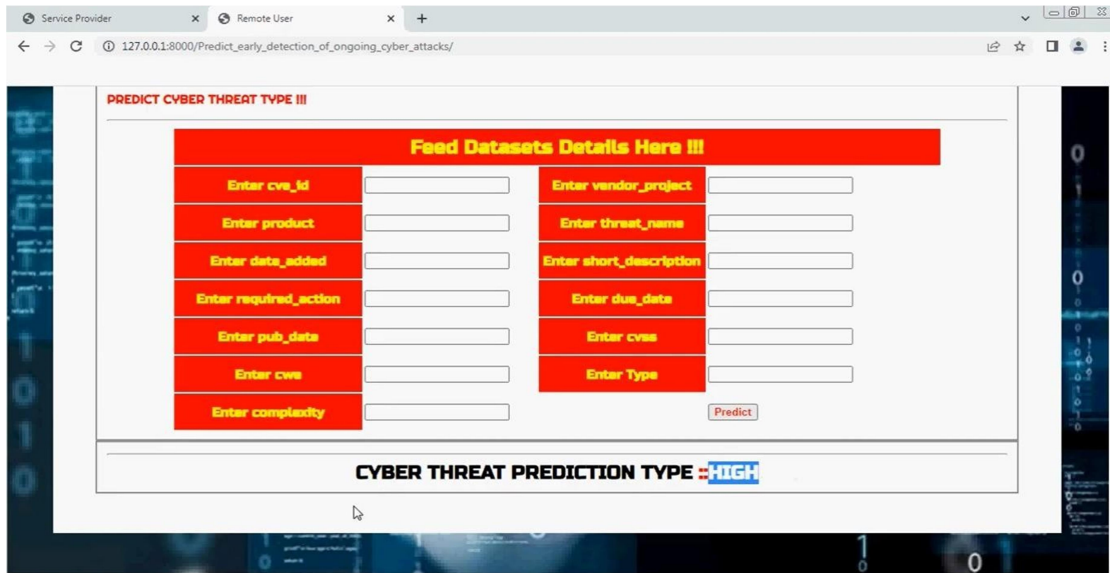
Enter cve_id	CVE-2016-0167	Enter vendor_project	microsoft
Enter product	Windows	Enter threat_name	Microsoft Windows Kernel W
Enter data_added	03-11-21	Enter short_description	The kernel-mode driver alloa
Enter required_action	Apply updates per vendor int	Enter due_data	03-05-22
Enter pub_date	12-04-16	Enter cvss	7.8
Enter cwe	CWE-264	Enter Type	LOCAL
Enter complexity	LOW		

**Predict**

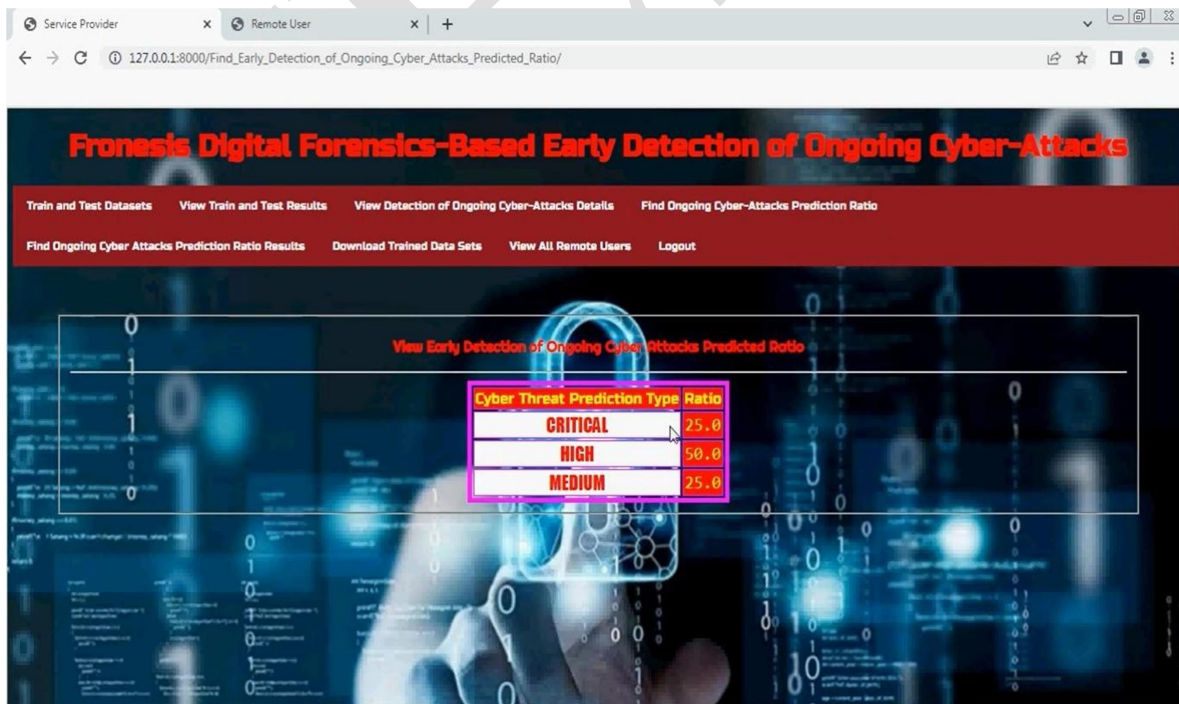
**CYBER THREAT PREDICTION TYPE ::**



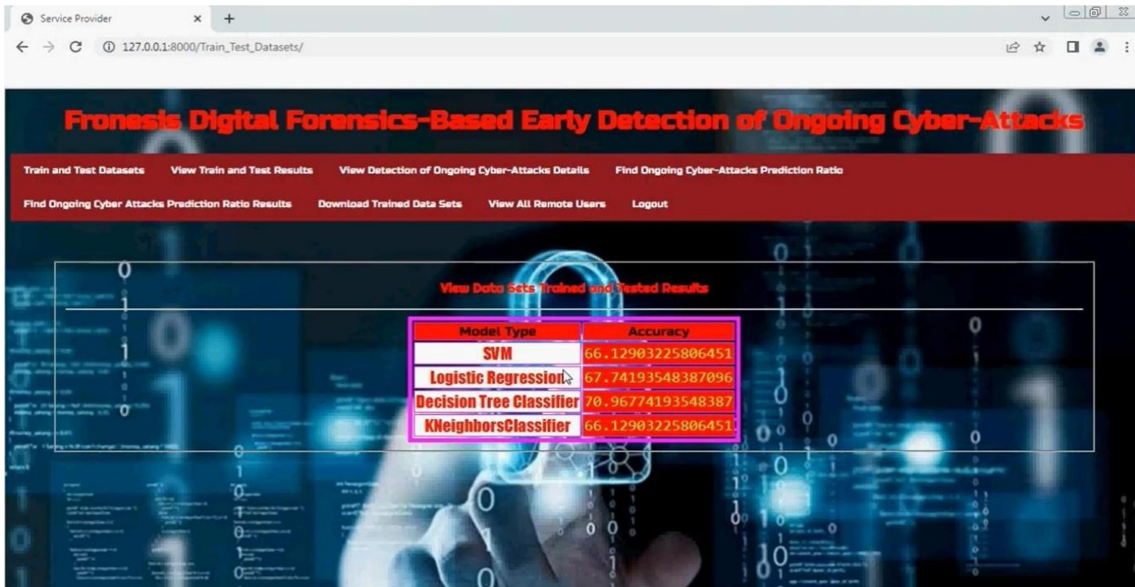
### PREDICTION OUTPUT



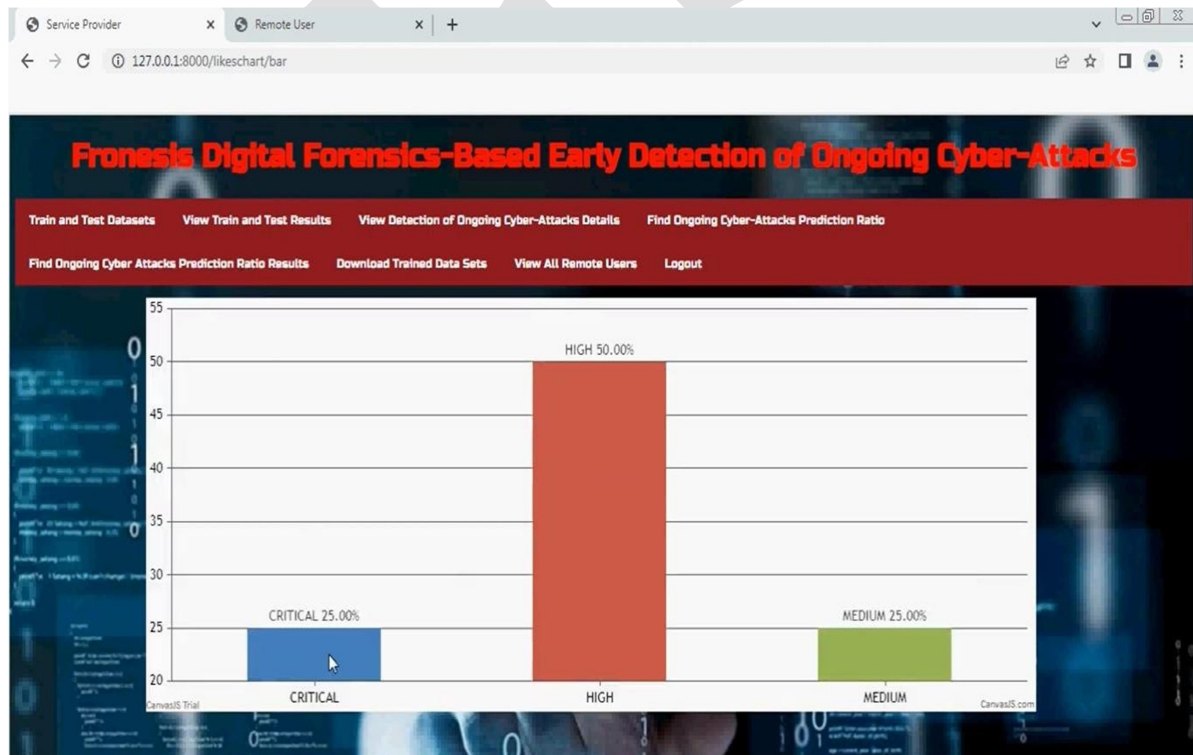
### VIEWING TRAINED AND TESTED RESULT



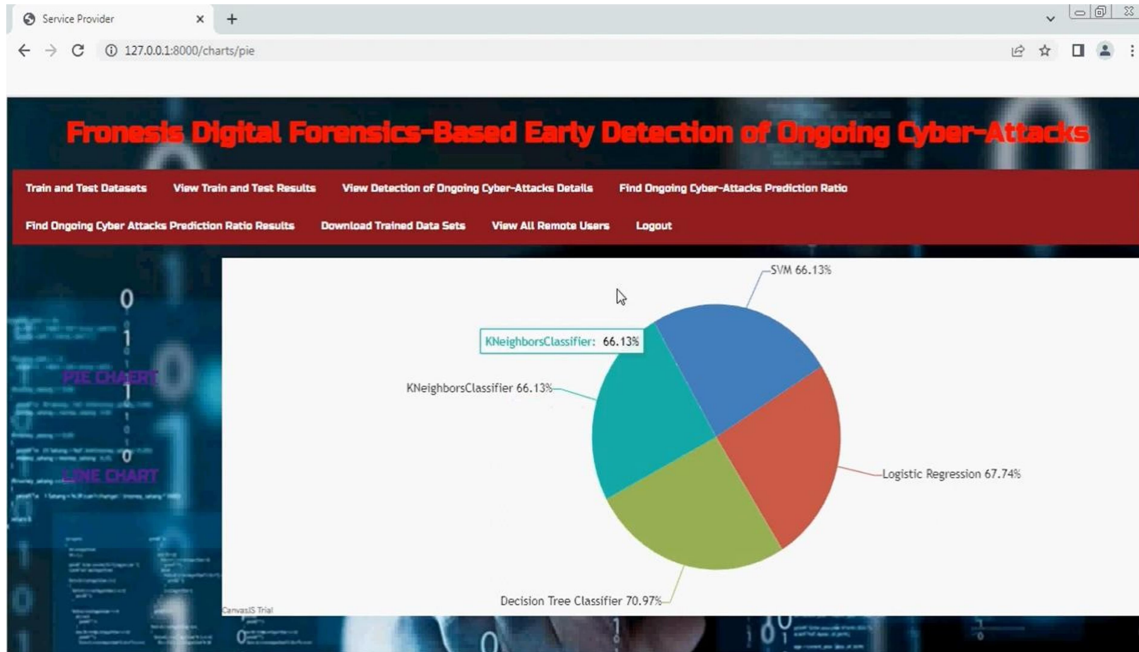
### VIEWING CYBER ATTACK RATIO



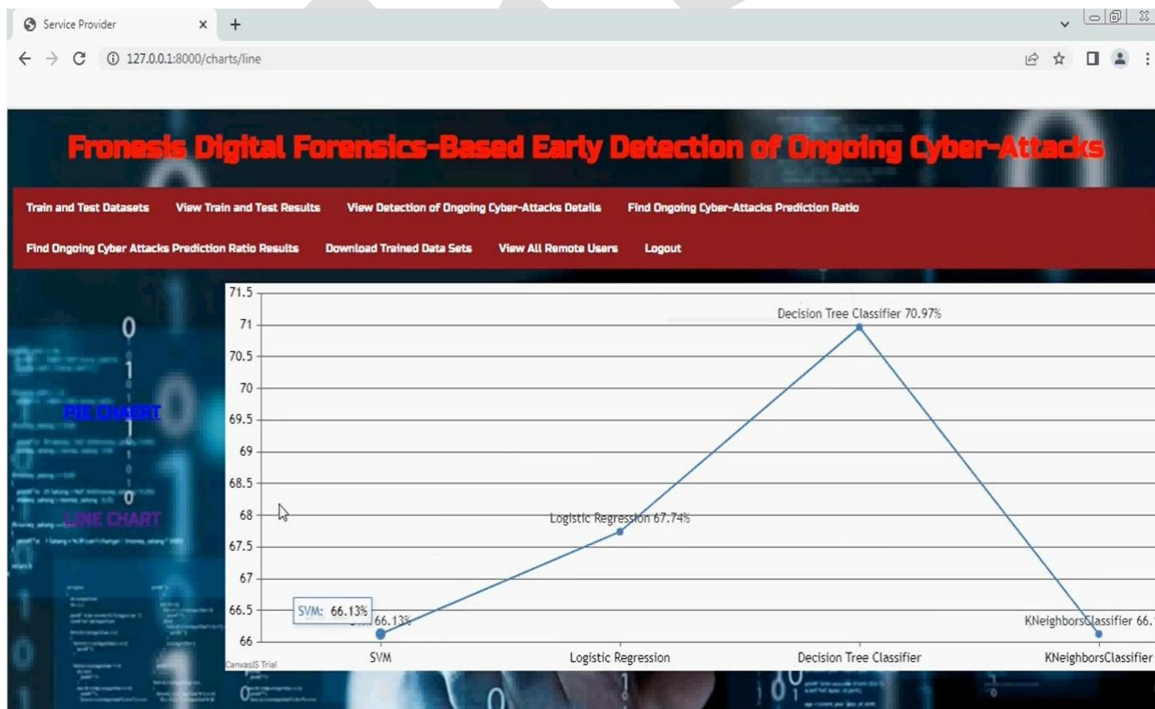
### BAR GRAPH



### PIE CHART



### LINE CHART



User training is necessary whenever a new system is built in order to educate users on how the system works, enabling them to effectively use it for its intended purpose. The project's functionality was shown to potential consumers for this specific objective. The functionality of the system is readily comprehensible, and its use is particularly straightforward given that the intended users possess a proficient understanding of computers.

This encompasses a broad spectrum of operations, including as rectifying code and design flaws. In order to minimize the need for future maintenance, we have refined the user's needs with greater precision throughout the system development process. This system has been created to meet the criteria to the greatest degree feasible. Advancements in technology may provide the incorporation of several more features in the future, depending on the specific needs and demands. The code and designing are straightforward and comprehensible, facilitating maintenance.

## CONCLUSION

This article introduces Fronesis, a cyber-attack detection technique that utilizes the MITRE ATT&CK knowledge base, Lockheed Martin's Cyber Kill Chain (CKC) intelligence model, and digital artifacts obtained from the monitored system. Digital artifacts are obtained using appropriate sensors in accordance with digital forensics protocols to guarantee the preservation of the integrity of the digital artifacts. Fronesis analyzes digital artifacts to identify MITRE ATT&CK methods by examining the distinctive patterns left behind by each technique's specific operations. The established methodologies are then linked with respective MITRE ATT&CK strategies, which are aligned with matching CKC stages. A continuous cyber-attack is identified by examining the artifacts of its stages and determining whether they are interconnected and arranged in the proper temporal sequence. Fronesis was implemented via the use of an ontology and rules, which were described using the Web Ontology Language (OWL) and the Semantic Web Rule Language (SWRL). This allowed Fronesis to function as a detection strategy based on rules. The ontology enables the representation of digital objects in a manner that can be easily exchanged and processed by computers. Meanwhile, the rules analyze the information about these artifacts to identify any ongoing cyber-attacks. MITRE ATT&CK, CKC, OWL, SWRL, and related rule-based reasoners are open source standards and technologies that facilitate widespread use of Fronesis.

The suggested detection technique may be implemented as an independent rule-based detection tool that analyzes the digital traces of the system it is deployed on to identify ongoing cyber-attacks. Furthermore, Fronesis has the capability to be included into digital forensics tools, therefore providing assistance in the examination of cyber-attacks. In this scenario, Fronesis will analyze the digital artifacts of a system to detect the occurrence of a cyber-attack, its evidence, as well as the specific MITRE ATT&CK methodologies, MITRE ATT&CK tactics, and CKC phases used. Our future study will focus on enhancing the computing efficiency of Fronesis in order to decrease the time required to identify a cyber-attack in progress. One may explore the use of big data technologies, such as Hadoop large data clusters, for optimization purposes.



## FUTURE ENHANCEMENTS

We are also directing our future efforts on evaluating Fronesis in terms of its effectiveness against cyber-attacks generated by MITRE Caldera [40]. Ultimately, it is important to examine the use of machine learning (ML) methods. For example, the Fronesis ontology may be used to establish similarity metrics for machine learning models, which can then be employed to find similarities across digital objects. The use of ML algorithms will be explored to automatically generate rules that may be employed in ontology-based reasoning to expand Fronesis. Latest technological breakthroughs will be considered in due course. In order to facilitate future projects, many components of the networking system will be designed in a generic manner throughout the technological build-up, allowing them to be easily used or integrated with other systems. The future promises many opportunities for the development and enhancement of this undertaking.

## REFERENCES

- [1] M. P. Barrett, "Framework for improving critical infrastructure cybersecurity, version 1.1," NIST Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. CSWP 04162018, Apr. 2018.
- [2] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, vol. 1. New York, NY, USA: Academic, 2011.
- [3] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 16\_24, 2013.
- [4] MANDIANT. M-Trends 2021: Insights Into Today's Top Cyber Trends and Attacks. Accessed: Sep. 5, 2021. [Online]. Available: [https://www.\\_reeye.com/current-threats/annual-threat-report/mtrends.html](https://www._reeye.com/current-threats/annual-threat-report/mtrends.html)
- [5] Ijteba Sultana, Dr. Mohd Abdul Bari, Dr. Sanjay, "Routing Performance Analysis of Infrastructure-less Wireless Networks with Intermediate Bottleneck Nodes", *International Journal of Intelligent Systems and Applications in Engineering*, ISSN no: 2147-6799 IJISAE, Vol 12 issue 3, 2024, Nov 2023
- [6] Md. Zainlabuddin, "Wearable sensor-based edge computing framework for cardiac arrhythmia detection and acute stroke prediction", *Journal of Sensor*, Volume 2023.
- [7] Md. Zainlabuddin, "Security Enhancement in Data Propagation for Wireless Network", *Journal of Sensor*, ISSN: 2237-0722 Vol. 11 No. 4 (2021).
- [8] Dr MD Zainlabuddin, "CLUSTER BASED MOBILITY MANAGEMENT ALGORITHMS FOR WIRELESS MESH NETWORKS", *Journal of Research Administration*, ISSN:1539-1590 | E-ISSN:2573-7104 , Vol. 5 No. 2, (2023)
- [9] Vaishnavi Lakadaram, "Content Management of Website Using Full Stack Technologies", *Industrial Engineering Journal*, ISSN: 0970-2555 Volume 15 Issue 11 October 2022
- [10]



- [11] Dr. Mohammed Abdul Bari, Arul Raj Natraj Rajgopal, Dr.P. Swetha, "Analysing AWSDevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution", International Journal of Intelligent Systems and Applications in Engineering, JISAE, ISSN:2147-6799, Nov 2023, 12(4s), 519–526
- [12] Ijteba Sultana, Mohd Abdul Bari and Sanjay, "Impact of Intermediate per Nodes on the QoS Provision in Wireless Infrastructure less Networks", Journal of Physics: Conference Series, Conf. Ser. 1998 012029, CONSILIO Aug 2021
- [13] M.A.Bari, Sunjay Kalkal, Shahanawaj Ahamad, "A Comparative Study and Performance Analysis of Routing Algorithms", in 3rd International Conference ICCIDM, Springer - 978- 981-10-3874-7\_3 Dec (2016)
- [14] Mohammed Rahmat Ali, "BIOMETRIC: AN e-AUTHENTICATION SYSTEM TRENDS AND FUTURE APPLICATION", International Journal of Scientific Research in Engineering (IJSRE), Volume1, Issue 7, July 2017
- [15] Mohammed Rahmat Ali, "BYOD... A systematic approach for analyzing and visualizing the type of data and information breaches with cyber security", NEUROQUANTOLOGY, Volume20, Issue 15, November 2022
- [16] Mohammed Rahmat Ali, "Computer Forensics -An Introduction of New Face to the Digital World", International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-453 – 456, Volume: 5 Issue: 7
- [17] Mohammed Rahmat Ali, "Digital Forensics and Artificial Intelligence ...A Study", International Journal of Innovative Science and Research Technology, ISSN:2456-2165, Volume: 5 Issue:12.
- [18] Mohammed Rahmat Ali, "Usage of Technology in Small and Medium Scale Business", International Journal of Advanced Research in Science & Technology (IJARST), ISSN:2581-9429, Volume: 7 Issue:1, July 2020.
- [19] Mohammed Rahmat Ali, "Internet of Things (IOT) Basics - An Introduction to the New Digital World", International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-32-36, Volume: 5 Issue: 10
- [20] Mohammed Rahmat Ali, "Internet of things (IOT) and information retrieval: an introduction", International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume: 7 Issue: 4, October 2017.
- [21] Mohammed Rahmat Ali, "How Internet of Things (IOT) Will Affect the Future - A Study", International Journal on Future Revolution in Computer Science & Communication Engineering, ISSN: 2454-424874 – 77, Volume: 3 Issue: 10, October 2017.
- [22] Mohammed Rahmat Ali, "ECO Friendly Advancements in computer Science Engineering and Technology", International Journal on Scientific Research in Engineering(IJSRE), Volume: 1 Issue: 1, January 2017
- [23] Ijteba Sultana, Dr. Mohd Abdul Bari, Dr. Sanjay, "Routing Quality of Service for Multipath Networks", International Journal of Intelligent Systems and Applications in Engineering", JISAE, ISSN:2147-6799, 2024, 12(5s), 08–16;

- [24] Mr. Pathan Ahmed Khan, Dr. M.A Bari, "Impact Of Emergence With Robotics At Educational Institution And Emerging Challenges", International Journal of Multidisciplinary Engineering in Current Research(IJMEC), ISSN: 2456-4265, Volume 6, Issue 12, December 2021,Page 43-46
- [25] Shahanawaj Ahamad, Mohammed Abdul Bari, Big Data Processing Model for Smart City Design: A Systematic Review ", VOL 2021: ISSUE 08 IS SN : 0011-9342 ;Design Engineering (Toronto) Elsevier SCI Oct : 021
- [26] Syed Shehriyar Ali, Mohammed Sarfaraz Shaikh, Syed Safi Uddin, Dr. Mohammed Abdul Bari, "Saas Product Comparison and Reviews Using Nlp", Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022
- [27] Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal,U K) Pages 1-6
- [28] .A.Bari& Shahanawaj Ahamad, "Managing Knowledge in Development of Agile Software", in International Journal of Advanced Computer Science & Applications (IJACSA), ISSN: 2156-5570, Vol: 2, No: 4, pp: 72-76, New York, U.S.A., April 2011
- [29] Imreena Ali (Ph.D), Naila Fathima, Prof. P.V.Sudha , "Deep Learning for Large-Scale Traffic-Sign Detection and Recognition", Journal of Chemical Health Risks, ISSN:2251-6727/ JCHR (2023) 13(3), 1238-1253
- [30] Imreena, Mohammed Ahmed Hussain, Mohammed Waseem Akram" An Automatic Advisor for Refactoring Software Clones Based on Machine Learning", Mathematical Statistician and Engineering Applications Vol. 72 No. 1 (2023)
- [31] Mrs Imreena Ali Rubeena, Qudsiya Fatima Fatimunisa "Pay as You Decrypt Using FEPOD Scheme and Blockchain", Mathematical Statistician and Engineering Applications: <https://doi.org/10.17762/msea.v72i1.2369> Vol. 72 No. 1 (2023)
- [32] Imreena Ali , Vishnuvardhan, B.Sudhakar," Proficient Caching Intended For Virtual Machines In Cloud Computing", International Journal Of Reviews On Recent Electronics And Computer Science , ISSN 2321-5461,IJRRECS/October 2013/Volume-1/Issue-6/1481-1486
- [33] Heena Yasmin, A Systematic Approach for Authentic and Integrity of Dissemination Data in Networks by Using Secure DiDrip, INTERNATIONAL JOURNAL OF PROFESSIONAL ENGINEERING STUDIES, Volume VI /Issue 5 / SEP 2016
- [34] Heena Yasmin, Cyber-Attack Detection in a Network, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)
- [35] Heena Yasmin, Emerging Continuous Integration Continuous Delivery (CI/CD) For Small Teams, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)