Cyber security & Ethical Hacking

Sreshtha Bhattacharya[1], Nida Khan[2], Garima Yadav[3], Tanushree Pandya[4]

[1]*Department of Computer Science & Engineering & Gyan Ganga Institute of Technology & Sciences ,Jabalpur*
[2]*Department of Computer Science & Engineering & Gyan Ganga Institute of Technology & Sciences ,Jabalpur*
[3]*Department of Computer Science & Engineering & Gyan Ganga Institute of Technology & Sciences ,Jabalpur*
[4]*Department of Computer Science & Engineering & Gyan Ganga Institute of Technology & Sciences ,Jabalpur*

Abstract— The paper presents a Fingerprint-Based Attendance Management System for university environments, addressing the challenges of impersonation, ghost worker syndrome, and student attendance management. The system enrolls and authenticates users by capturing their fingerprints and extracting distinctive minutiae points for identification. The data is stored in a database, and the system then verifies identity before marking attendance. Implemented with Microsoft's C# and SQL Server 2005, the system has a 97.4% accuracy level, providing a secure and reliable solution to prevent impersonation.This research paper explores ethical hacking and penetration testing within the context of today's cybersecurity landscape. In the current world where cyber attack has become serious issue. Ethical hacking, which can be studied prior and then applied on real world applications and software so that the data cannot be exploited and misuse. By conducting survey and doing research we have found many new tools and technique that are used in ethical hacking

Keywords— Ethical Hacking, Penetration Testing, Cyber security, Security Threats, Vulnerability Assessment, Ethical Hacking Education, Information Security Training, Cyber Defense Learning

Graphical Abstract- Due to the significant financial losses, brand damage, erosion of consumer trust, and personal consequences caused by fraudulent activities, businesses, governments, and individuals increasingly recognize the importance of information security. Given the seriousness of these issues, students pursuing careers in this field should acquire degrees that prepare them to engage effectively with the broader user community. Ethical hacking education equips future professionals with the knowledge and skills necessary to address current and emerging cybersecurity challenges. This study aims to define ethical hacking, examine current trends in information security, explore effective teaching methods, review training practices, and highlight best practices within the discipline

Background- The history of hacking will be briefly discussed in order to better understand the need for constructive steps relating to the education of potential security professionals. Hacking originated in the 1960s, primarily at the campuses of the Massachusetts Institute of Technology (MIT) and Stanford University. At the time, the term "hack" applied to code shortcuts and was thought to be a more effective way to complete tasks.
Recent cybersecurity incidents are alarming, and they demonstrate that today's cybersecurity practitioners must take a more proactive approach to protection. Although there are more cybersecurity incidents on the rise, there have been some high-profile attacks in the news in the last year that necessitated advanced technological expertise. The 2016-2017 Democratic National Convention hack (DNC Hack),

1. Introduction

In a generation of digital change where every person and devices are connected to each other, the cyber security has become the important aspect of our life and data. With the technology upgrading itself the threats are also increasing day-by day. So, the ethical hacking and penetration testing have become a tool for finding vulnerability and cyber threats. One often thinks that these two terms are synonyms of each other. However, that is not the case. The main motive behind penetration testing is to find out the vulnerability and report it to the

concerning authority before the criminal exploits it. Whereas Ethical hackers study the whole security system of the company. But their work is not limited up to finding vulnerabilities; they also suggest solutions for solving them. In this paper we will also cover what is hacking, types of hackers, how can we protect our self, tools used for ethical hacking, methods of attack, different phases of hacking, legal implications, prerequisites for becoming ethical hacker, career opportunities. Moreover, we will also mention the new trends such as Bug bounty program, and Hackathons.

1.1 Methodology

1.1.1 What is Hacking?

Hacking is a technique which includes compromising computers or devices to gain the access, this access can be authorize or unauthorize depending on the intention of the hackers. The hackers find loopholes or weakness in the systems or networks to gain entry for the exploitation of data. Many Organizations hire these hackers to find the weakness in their own systems. This paper examines the stages of hacking, associated legal and ethical considerations, the qualifications required to become an ethical hacker, and related career opportunities. For better understanding let us term them as righteous and malicious hackers. Righteous hackers- These hackers aim to report the vulnerabilities they found in the system for the protection of organization for example- penetration testers. Malicious hackers- These hackers exploit the vulnerabilities they found for their own benefit for examplecybercriminalsThis approach aims to:

1.1.2 Types of Hackers-

1. **White Hat Hackers**- These are the individuals who use their hacking techniques for valid reasons. They are usually appointed by companies or organizations to test and eradicate the vulnerabilities in their systems. These white hat hackers execute vulnerability assessments, penetration testing and review the security policies of the organizations or companies. These hackers are generally driven to safeguard systems from cyber-attacks. These are also called as ethical hackers.

2. **Black Hat Hackers**: Black hat hackers are malicious hackers who are involved in illegal work to gain entry in networks and systems. They are mostly involved in activities consisting of stealing personal information, selling them on dark web and ransomware attacks. These hackers are generally related with criminal activities. Black hat hackers are inspired by personal revenge, financial profit or just to cause harm and destruction.

3. **Grey Hat Hackers:** These hackers work in between white hat and black hat hackers. They don't have any wrong intent but they don't have proper permissions from the owners to access their systems and networks. Grey hat hackers may find vulnerabilities and notify the affected organization, but they mostly do it without taking permission from the organization

1.2 Phases of Ethical Hacking

1. **Foot Printing** :Foot printing is the very first step which hacker uses. In this process hacker tries to gather all the information of the targeted organizations or victims. This part is also called as information gathering. It can generally be done in two ways first is gathering information available publicly and the second way is by communicating with the selected system. Hackers uses various online tools to gather publicly available information such as WHOIS lookups, this tool helps to find the detailed information about ip address and domain names.

2. **Scanning and Enumeration**:After collecting the information from the step one, Hacker moves on to the second step which is Scanning and Enumeration. In this step hacker tries to find out the loopholes or any weaknesses in the system or network through which he can get the entry point. Attackers use tools like network scanners like Wireshark and Nmap to find open ports, services running on those ports, and potential flaws. This step also includes withdrawing information of the targeted system, for examples user version of the software's, details about the operating systems. This step is very crucial for hacker as critical for identifying vulnerabilities.

3. **Gaining Access:** This phase is the main objective of the hacker as the actual intrusion starts from this phase Once vulnerabilities or weaknesses are found, the hacker tries to get into the loophole of the system without any permission [Unauthorized Way]. The hacker starts using various methods for getting into the system. This method consists of various techniques like SQL Injection, Bypassing the authentication present in the system, bypassing firewall security, escaping intrusion detection systems. The aim of the hacker is to obtain the proper access of the systems.

4. **Maintaining access:** Once the hacker successfully gets the access of the system, the main objective is to maintain and control the compromised system for a long period of time. The hacker makes sures that he has continued access to carry out further malicious attacks on the systems. Hacker generally creates the backdoor in the systems which will allow them to re-enter the system again without performing the same process again. To avoid being getting detected hackers continuously monitor the system and network through which they have gained the access.

5. **Clearing the tracks**: This is the final step a hackers must not forget before leaving the system. That is clearing the tracks. In this final step, hackers should aim to focus on covering their tracks to avoid getting detected by cyber security professionals and system admins. They should generally destroy the proof of their appearance in the systems and all the activities perform by them, by deleting all the log files and history. This is a very important part for avoiding being caught which may cause them future legal problems.

1.3 EXISTING MODELS IN CYBERSECURITY

1. Hashed Password Cracker: The hashed password cracker tool is a user-friendly tool designed to crack secure passwords using brute force, dictionary attacks, and rainbow table lookups. It offers a user-friendly interface for inputting hashed passwords and employs advanced algorithms for efficiency and speed. The project aims to assist users in recovering forgotten passwords or testing the strength of their hashed password implementations.

2. Optimized Password Cracker: The password cracker tool will use advanced techniques and algorithms like MD5, SHA-1, and bcrypt to crack encrypted passwords. It will use parallel processing and GPU acceleration to increase speed and efficiency. The tool will also offer customizable options for dictionary, brute-force, and hybrid attacks. The goal is to provide a high-performance, versatile tool for retrieving lost passwords or evaluating password implementation strength.

3. File Type Identification Using The Magic Number: The project aims to create a file-type identification tool using magic numbers, which are unique byte sequences at the beginning of files, to accurately identify their file formats, regardless of their extension, by scanning and analyzing these numbers.

Magic Number	File Extension	Converted to Text
474946383961	GIF Files	GIF89a
526172211A0700	RAR Files	Rar!##
89504E470D0A1A0A	PNG Files	‰PNG
255044462D	PDF Files	%PDF-
D9B48EF9	Bitcoin Block	

4. Cloud Access Security Broker (CASB): CASBs provide visibility and administrative control for businesses with multiple SaaS apps. Cloud application discovery can uncover hidden IT resources, validating projects. Leaders can assess visibility and control over sensitive data shared by SaaS apps and determine the required level for each cloud service. Short-term contracts should focus on data discovery and security.

5. Authentication Of User Using Facial Acknowledgement: A facial acknowledgment framework can be created for client confirmation, utilized in exam proctoring frameworks, KYC preparing frameworks, and portable gadgets. The framework has records of the aiming user's photos, which can be open or confined to particular clients. After camera authorization is allowed, the confront is recognized and coordinated with pictures in its database. The program peruses the geometry of the confront, such as remove between eyes, profundity of eye attachments, and shape of cheekbones, lips, ears, chin, and nose. This information is changed over into a numerical code called faceprint, which is at that point coordinated with existing faceprint within the framework. The net confront finder can moreover be planned for seeing faces in video calls. This extend can be expanded for utilize cases like client confirmation in gatherings, exams, police powers, and phone confront open highlights.

2. PROPOSED MODEL

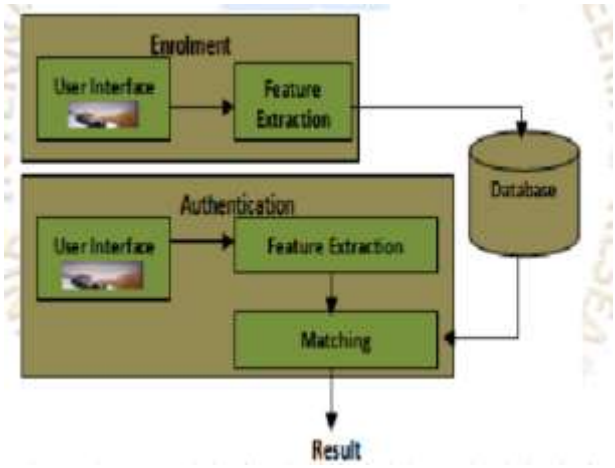
2.1. Introduction: The paper explores the use of biometric technologies in identity verification, particularly fingerprint identification, to address challenges like impersonation and student attendance. It highlights the uniqueness and stability of fingerprint identification, and proposes An Attendance system based on Fingerprint technology to provide an effective identity management solution.

2.1.2. Attendance Management: Attendance management is crucial for reducing workforce downtime and promoting productivity. Traditional methods like

time clocks and timesheets have limitations, leading to the use of automated solutions. The paper categorizes attendance management into conventional and automated methods, emphasizing the advantages of biometric systems, particularly fingerprints.

2.1.3 Related Works: The paper discusses attendance management systems, exploring technologies like RFID, face recognition, and iris recognition. However, existing systems face limitations like impersonation, installation issues, and high financial burdens. The paper proposes a Fingerprint-Based Attendance Management System for a secure, reliable, and convenient solution.

3. System Overview: The proposed system uses a database for enrolment and authentication, extracting minutiae points from user fingerprints and storing them as templates. Authentication involves comparing captured features with stored templates to verify identity. Implemented using Microsoft's C# and SQL Server 2005, it achieved a 97.4% accuracy rate.



4. Architecture:

An Attendance system based on Fingerprint technology is designed with meticulous attention to detail, capturing biometric data and user information through two image samples per fingerprint. The minutiae extraction process uses the Crossing Number method, while the authentication phase ensures accurate identity verification, contributing to the system's overall security.

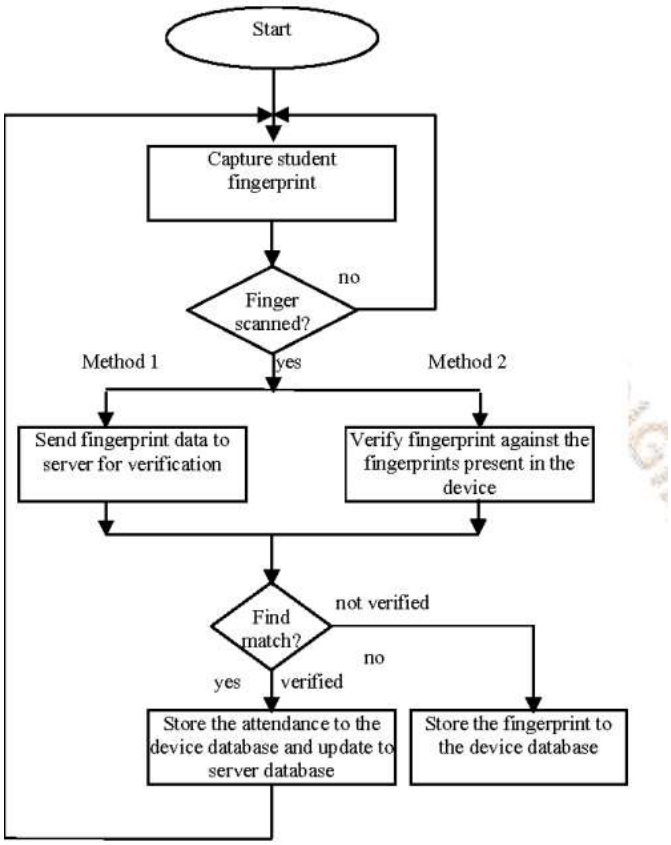


Fig. 3. Flow chart of the system operation.

5. Results :

Cybersecurity is a critical aspect of the digital era, serving as the vanguard against evolving cyber threats. As our dependence on digital infrastructure grows exponentially, the future scope of cybersecurity becomes expansive and pivotal. The integration of cutting-edge technologies such as artificial intelligence, machine learning, and quantum computing will enable the creation of sophisticated intrusion detection systems, predictive threat analysis mechanisms. The future of cyber security is crucial for securing critical infrastructures, as societies become more reliant on digital ecosystems for essential services like energy, healthcare, and finance. Protecting critical infrastructure requires a multidimensional approach that combines technological innovation with strategic policy frameworks. Governments and organizations must collaborate to establish robust cyber defense strategies and international agreements to mitigate the risks posed by state-sponsored cyber threats and cyber warfare. Educational institutions and training programs must adapt to this evolving landscape, providing students with hands-on experiences and real-world scenarios to hone their cyber security skills. The role of cyber security professionals will extend beyond mere technical expertise, encompassing a comprehensive understanding of legal,ethical,social implications. The future of cyber

security is intricately linked to privacy concerns and ethical considerations. As technologies like surveillance systems, biometrics, and facial recognition become integral to security measures, there is a delicate balance to strike between safeguarding individual privacy rights and ensuring public safety. Policymakers will grapple with the formulation of regulations and standards that strike this balance, with ethical considerations guiding technologies. In conclusion, the future scope of cybersecurity is expansive and critical in an era dominated by digital transformation. It involves the integration of advanced technologies, global collaboration, the development of a skilled workforce, and a nuanced approach to ethical considerations

6. Conclusion and Future Scope

The Fingerprint-Based Attendance Management System is a promising solution for managing impersonation and attendance in universities. Its efficiency, accuracy, and security make it a valuable tool for educational institutions and organizations. The system's success in preventing impersonation and time-saving benefits make it a valuable tool for biometric-based attendance systems, showcasing the potential for secure identity verification in various sectors.

7. Acknowledgement-. My heartfelt appreciation goes to my Dean for his constructive feedback and collaborative spirit **Dr.Ashok Verma, Dean,CSE,** for his invaluable guidance and unwavering support throughout this project. His expertise in computer vision and pattern recognition was instrumental in overcoming numerous technical challenges.

8. References

Cybersecurity-Future Scope, Rekha.R[1],Akshita.R[2], Anukraha.T.V[3],Annie Rufina.C4 , Monica.N5 ,Abinaya Sree A.B.

CYBERSECURITY IN THE MODERN WORLD: ETHICAL HACKING Saachi Joshi*1, Khushal Chauhan*2, Mayur Ghawate*3, Sejal Kulkarni*4

https://www.researchgate.net/publication/383529875_Ethical_Hacking_and_its_role_in_Cybersecurity

Bratus, S., & Masone, C. (2007). Hacker Curriculum: How We Can Use It in Teaching]. IEEE Distributed Systems Online, 8(11), 1-5. doi:10.1109/mdso.2007.61.

D. Acharya and A. K. Mishra, "Wireless Fingerprint based Student Attendance system", National Institute of Technology Rourkela, 2010. http://ethesis.nitrkl.ac.in/1765/

C. Saraswat, C. et al, "An Efficient Automatic Attendance System using Fingerprint Verification Technique". International Journal on Computer Science and Engineering. 2(02):264-269, 2010

S. Pankanti, S. Prabhakar, and A.K. Jain, "On the Individuality of Fingerprints". IEEE Transaction on Pattern Analysis and Machine Intelligence.24(8), 200

O. Shoewu and O. Badejo, "Radio Frequency Identification Technology: Development, Application and Security Issues". Pacific Journal of Science and Technology. 7(2):144-152,.2006

T. Nawaz, S. Pervaiz, and A.K. Azhar-Ud-Din, "Development of Academic Attendance Monitoring System Using Fingerprint Identification".2009

Sravan Kumar Challa, Akhilesh Kumar, and Vijay Bhaskar Semwal. A multibranch cnn-bilstm model for human activity recognition using wearable sensor data. The Visual Computer, 38(12):4095–4109, 2022.

AUTHORS PROFILE

Sreshtha Bhattacharya- earned his B. Tech in Information Technology, from HCET in 2008 ,Jabalpur M. Tech.in Computer Technology & Architecture from GGITS in 2015,Jabalpur respectively. She is currently working as Assistant Professor in Department of Computer Science & Engineering from GGITS, Jabalpur since 2008. She has published more than 10 research papers in reputed international journals and conferences including IEEE and it's also available online. Her main research work focuses on Engineering & Technology, IoT,Machine Lerning and Computational Intelligence. She has 15 years of teaching experience and 10 years of research experience.

Nida Khan- earned his B. Tech in Computer Science, from Global Engineering College in 2020 ,Jabalpur M. Tech.in IoT from GGITS in 2024,Jabalpur respectively. She is currently working as Assistant Professor in Department of Computer Science & Engineering(IoT) from GGITS, Jabalpur since 2025. She has published more than 4 research papers in reputed international journals and conferences including IEEE and it's also available online. Her main research work focuses on Engineering & Technology, IoT,Machine Lerning and Computational Intelligence. She has 4 years of teaching experience and 1 years of research experience.