International Journal of Scientific and Management Research
Volume 8 Issue 5 (May) 2025
ISSN: 2581-6888
Page: 177-198

The Role of Artificial Intelligence in Strengthening Privacy and Security in the Era of Cyber Crime and Digital Forensics

Victoria Abosede Ogunsanya, Rianat Abbas, Laticbe Elijah, Joy Awoleye, Adetomiwa Adesokan, Kumbirai Bernard Muhwati, & Average Guma
Cybersecurity Analyst, University of Bradford, UK
Information Systems, Baylor University, Texas, USA
Cybersecurity, Yeshiva University, New York, USA
Cybersecurity, Yeshiva University, New York, USA
Computer Science, Yeshiva University, New York, USA
Cybersecurity, Yeshiva University, New York, **USA**

DOI - http://doi.org/10.37502/IJSMR.2025.8515

Abstract

This study explores the role of Artificial Intelligence (AI) in strengthening privacy and security amidst the growing challenges of cybercrime and digital forensics. As cyber-attacks become more sophisticated, traditional methods of securing sensitive data and investigating digital crimes are increasingly inadequate. This research examines the use of machine learning algorithms, particularly Random Forest Classifier (RFC) and Gradient Boosting Classifier (GBC), in detecting network anomalies and enhancing the detection of cyberattacks. The study also highlights the critical need for AI-driven techniques to support digital forensic investigations by providing more accurate and efficient methods of identifying malicious activities. Using a dataset of network traffic features, the study reveals the class imbalance between normal and attack traffic, which can hinder detection accuracy. Despite this imbalance, both RFC and GBC achieved perfect classification with AUC scores of 1.00. GBC, however, outperformed RFC in accuracy (91.3%), precision (91.4%), and recall (91.3%), demonstrating its superior ability to identify attack traffic while preserving privacy. Feature importance analysis found that Average Packet Size and Fwd Packets Length were the most significant indicators of attack behavior. The findings underscore the importance of AI in enhancing cybersecurity systems, ensuring robust privacy protections, and advancing digital forensic capabilities. The study also emphasizes the need for continuous model retraining, class balancing, and hyperparameter tuning to adapt to evolving threats. These AI-driven approaches have the potential to transform the landscape of digital forensics and cybersecurity, offering more resilient defenses against cybercrime and safeguarding privacy in an increasingly digital world.

Keywords: Artificial Intelligence, Cybercrime, Digital Forensics, Privacy Protection, Machine Learning, Random Forest Classifier, Gradient Boosting Classifier, Cybersecurity, Attack Detection, Feature Importance, Model Evaluation

1. Introduction

The rapid development of digital technologies has brought about unprecedented connectedness and convenience and has also given rise to more complex cyber-threats that challenge conventional security paradigms (Sagar et al., 2019). Also, Kaur et al. (2023) asserted that artificial intelligence (AI) has become a vital ally in the continuous fight to safeguard privacy and improve security against changing cybercrime strategies and redirecting the angle from which malicious activity is seen in the digital world, thereby resulting in a complete change as a result of the convergence of AI, cybersecurity, and digital forensics. The security community has switched to intelligent systems that can learn, adapt, and react in real-time to these new threats as cybercriminals use increasingly sophisticated tactics, such as AI-powered phishing schemes and sophisticated malware that avoids traditional detection (Bhat et al., 2024).

Furthermore, artificial intelligence (AI) refers to computer programs created to carry out operations like learning, reasoning, and decision-making that normally call for human intelligence (Yadav, 2024). However, Bayan (2024) expressed that AI systems can recognize intricate patterns, anticipate possible dangers, and automate intricate procedures with remarkable accuracy by using machine learning algorithms and data analysis. The study further stated that AI improves cybersecurity by continuously scanning networks for irregularities, identifying malware instantly, and stopping data breaches before they happen. Artificial Intelligence (AI) speeds up investigations in digital forensics by processing large volumes of digital evidence quickly, reconstructing attack timelines, and uncovering hidden connections in cybercrime cases (Hassan & Ibrahim, 2023).

Additionally, AI is especially useful in today's data-intensive environment because it can process and analyze enormous amounts of data at speeds that are impossible for human operators (Lami, et al., 2024). Also, Ezeji (2024) opined that while natural language processing can keep an eye out for social engineering attempts in communications, machine learning algorithms can spot minute patterns and irregularities in network traffic that could point to a breach attempt. However, Stewart (2023) highlighted that by automating the analysis of digital evidence, these technologies are not only transforming threat detection but also digital forensics, sometimes cutting down investigation times from weeks to hours. Proactive defense mechanisms are made possible by AI systems' predictive capabilities, which enable organizations to foresee and address possible vulnerabilities before they can be exploited (Akhtar et al., 2022).

In the same vein, the applicability of AI in cybersecurity is relevant in a variety of fields, such as financial services, where it can identify fraudulent transactions; healthcare, where it can safeguard private patient information; and critical infrastructure, where it can prevent potentially disastrous attacks. In the field of digital forensics, artificial intelligence (AI) helps investigators sift through terabytes of data, find pertinent evidence, and even accurately recreate digital crime scenes (Abbas et al., 2025). With the proliferation of Internet of Things (IoT) devices and cloud computing services, the volume and complexity of digital evidence continue to grow exponentially, making these capabilities especially important.

However, integrating AI into security frameworks is not without its challenges, one of which is Algorithmic bias, the possibility of adversarial attacks against AI systems, and the transparency of AI-driven decisions must all be carefully considered (Faqir, 2023). Also, Binhammad et al. (2024) stated that the same AI technologies that protect systems can also be weaponized by malicious actors, leading to an ongoing arms race in the cybersecurity space, and privacy concerns are a major concern, as the comprehensive data collection needed for AI security systems must be weighed against individual rights and legal requirements like the CCPA and GDPR (Mohammadiounotiki & Babaeitarkami, 2024).

Additionally, Ali et al. (2022) stated that defensive strategies have had to change in tandem with the evolution of cyber threats, with artificial intelligence leading the way. The study further highlighted that artificial intelligence (AI)-powered solutions are raising the bar for security efficacy, from behavioral biometrics that verify users based on their typing habits to deep learning models that identify zero-day exploits. AI in digital forensics is helping investigators keep up with the increasingly sophisticated cybercriminals who are using the dark web, anonymization methods, and encryption to hide their activities (Alghamdi, 2020). Furthermore, the increasing reliance of society on digital systems for everything from national security to financial transactions makes these developments especially important. To this end, the study seeks to assess how artificial intelligence (AI) improves cybersecurity threat detection and response systems, allowing for automated attack mitigation, real-time cyber threat identification, and enhanced forensic analysis to counteract changing cybercrime strategies.

2. Literature Review

Artificial Intelligence (AI) has become a key instrument for improving security and privacy, especially in thwarting changing cyberthreats and advancing digital forensics (Binhammad, et al., 2024). However, the study conducted by Hassan & Ibrahim (2023) shows that artificial intelligence (AI) can reduce vulnerabilities that rely on humans by improving encryption, automating incident response, and thwarting social engineering attacks. Nonetheless, issues like hostile AI attacks and moral dilemmas continue to exist, necessitating strong governance structures (Bayan 2024). This review critically examines six key concepts that address the research themes in order to assess the transformative potential of AI-driven cybersecurity, forensic efficiency, and risk mitigation.

2.1. Artificial Intelligence-Powered Threat Detection & Prevention

In the face of growing cybercrime, threat detection and prevention driven by artificial intelligence (AI) is transforming how businesses protect security and privacy (Lami, Hussein, Rajamanickam, & Emmanuel, 2024). Also, Alghamdi (2020) asserted that AI systems are far more capable than conventional security measures at identifying and thwarting threats in real-time by utilizing machine learning algorithms and advanced analytics. By detecting anomalies, anticipating possible attacks, and automating responses, these systems reduce the window of vulnerability by analyzing enormous volumes of data. However, Madhumitha (2024) expressed that AI is able to identify patterns that point to insider threats, malware, or phishing, allowing for preventative action before serious harm is done. In a time when cybercriminals are using more complex strategies to take advantage of weaknesses in digital systems, this ability is essential.

Furthermore, AI improves digital forensics by finding hidden evidence in complex datasets (Singh & Bahuguna, 2023). However, Priyadharshini et al. (2025) established that the complexity of digital evidence left behind by cyberattacks is too great for traditional methods to handle. Artificial intelligence (AI)-driven solutions can swiftly correlate data from multiple sources, reconstructing attack timelines and identifying the perpetrators. This expedites inquiries while upholding privacy norms because AI-powered tools can adjust to evolving threats; they are essential in the fight against cybercrime (Lami et al., 2024). Also, adherence to data protection regulations such as the CCPA and GDPR is addressed by AI's incorporation into security and privacy frameworks. AI systems can reduce breaches and human error by enforcing access controls, monitoring data flows, and identifying unauthorized disclosures (Singh & Bahuguna, 2023).

Additionally, Patil (2024) investigates artificial intelligence (AI) in cybersecurity, using data analytics and machine learning (ML) to enhance threat detection and prevention using supervised and unsupervised learning models that have been trained on sizable datasets. While acknowledging limitations like its reliance on high-quality, labeled data, which may not always be available, the study emphasizes AI's capacity to detect anomalies and anticipate attacks. Significant difficulties are also presented by adversarial attacks that target AI models and ethical worries about data privacy (Singh & Bahuguna, 2023). Although Dunsin et al. (2024) noted that computational expenses and the requirement for frequent model updates to accommodate changing threats are also mentioned in the study. These limitations imply that although AI improves cybersecurity, hybrid strategies and human oversight are still necessary for strong defenses.

2.1.1 Artificial Intelligence in Digital Forensics & Incident Response

Digital forensics and incident response are two fields where artificial intelligence (AI) is revolutionizing the detection, analysis, and mitigation of cyberthreats (Dunsin et al., 2024). Matsaung & Masiloane (2024) highlighted that AI offers a crucial advantage in a time when cybercrime tactics are changing quickly by automating the gathering and analysis of massive amounts of digital evidence, facilitating quicker and more precise investigations. Compared to manual methods, artificial intelligence (AI) systems can significantly improve the efficiency and depth of forensic analysis by using machine learning algorithms to detect patterns of malicious behavior, correlate events across multiple data sources, and identify anomalies (Abbas et al., 2025).

Similarly, through the automation of decision-making and real-time threat detection, artificial intelligence (AI) is transforming cybercrime and empowering businesses to react to cyberattacks with speed and precision (Faqir, 2023). Also, Binhammad et al. (2024) expressed that Systems with AI capabilities can rank alerts, spot suspicious activity, and start containment measures. This prompt action lessens the impact of security breaches, particularly as hackers employ increasingly complex techniques. However, Kaur et al. (2023) opined that constant learning from new occurrences and offering proactive recommendations improves threat intelligence by automating the detection of illegal access and data exfiltration and enforcing privacy-preserving measures like data anonymization. Hope (2024) also noted that it helps to improve security and privacy. AI supports ethical standards and legal frameworks while also improving cybercrime technology.

Furthermore, in order to evaluate the role of Artificial intelligent and Machine Learning models such as deep learning and ensemble methods in digital forensics and incident response (DFIR), Dunsin et al. (2024) use a mixed-methods approach that combines a systematic literature review with experimental validation of these models. The study emphasizes how well AI can automate malware detection and evidence analysis, but it also points out drawbacks like dataset bias that could distort model performance in practical settings. Transparency in legal contexts

Copyright © The Author, 2025 (www.ijsmr.in)

is also hampered by the difficulty in interpreting complex AI models. Key limitations are also identified by the study as being computationally demanding and susceptible to adversarial manipulations of forensic data. These drawbacks highlight how hybrid human-AI frameworks are required to guarantee accountability and dependability in DFIR procedures.

2.1.2 Artificial Intelligence for Privacy Preservation

Artificial intelligence (AI) is essential to protecting privacy because it makes it possible to employ sophisticated methods that preserve sensitive information without sacrificing usability (Hassan & Ibrahim, 2023). However, Sharma (2021) highlighted that traditional privacy protection techniques, like access controls and encryption, are frequently inflexible and find it difficult to adjust to changing threats. Artificial Intelligence (AI) improves these techniques by using machine learning to identify and anonymize personal data instantly, guaranteeing adherence to privacy laws such as the CCPA and GDPR. Furthermore, Stewart (2023) avowed that AI-powered solutions can automatically remove personally identifiable information (PII) from databases, videos, and documents, reducing the risk of exposure. Moreover, controlled noise is added to datasets by AI-driven differential privacy techniques, enabling organizations to share aggregated insights without jeopardizing individual identities. This harmony between privacy and data utility is essential in industries like healthcare and finance, where sensitive data must be safeguarded without impeding innovation; striking a balance between data utility and privacy is essential (Lami et al., 2024).

In like manner, digital forensics relies heavily on artificial intelligence (AI) to make sure investigations follow the law and ethical standards (Yadav, 2024). Also, Sharma (2021) argued that AI can speed up the process and lower privacy violations by eliminating unnecessary information and concentrating on pertinent evidence. Although the study conducted by Akhtar et al. (2022) expressed that while strict access controls guarantee that only authorized individuals handle sensitive data, AI algorithms can automatically blur faces in surveillance footage or omit irrelevant communications. As a result, digital forensic processes are more effective and trustworthy. Algorithmic bias and an over-reliance on automated procedures are two disadvantages of AI, though (Iwuh & Sonubi, 2024). To lower risks and guarantee accountability, Yadav (2024) stated that organizations need to put in place transparent and auditable AI frameworks. When applied correctly, artificial intelligence (AI) can be a powerful ally in the fight against cybercrime by offering robust privacy protections without sacrificing security.

Additionally, using case studies and comparative analysis, Khalid et al. (2023) perform a systematic review of privacy-preserving AI methods in healthcare, such as federated learning, homomorphic encryption, and differential privacy, and assess their efficacy. The research emphasizes their potential for protecting private medical information, but it also points out drawbacks like computational overhead that may prevent real-time implementation in clinical settings. Additionally, it is still difficult to balance model accuracy with privacy guarantees, especially in intricate deep learning applications. Additionally, the authors point out interoperability and regulatory obstacles to the widespread adoption of these methods in various healthcare systems. In AI-driven healthcare applications, these limitations highlight the need for well-rounded solutions that maximize privacy and performance.

2.1.3 Behavioral Analytics

Artificial intelligence-driven behavioral analytics has become a potent instrument for enhancing security and privacy in the digital age, especially in the fields of digital forensics and cybercrime (Hope, 2024). Also, Jones et al. (2025) expressed that AI-driven behavioral analytics can create a baseline of typical activity for every user or system by examining user behavior patterns, including login times, access locations, and typical data usage. When this standard is broken, it may indicate possible dangers like insider threats, account compromise, or illegal access attempts (Faqir, 2023). In order to detect subtle or complex attacks that could elude conventional rule-based security systems, proactive monitoring is essential (Hope, 2024).

Furthermore, behavioral analytics improves digital forensics by offering contextualized insights into user behavior both before and after security incidents. Reconstructing timelines, spotting questionable patterns of behavior, and correlating actions across systems or user accounts are all made easier by AI algorithms (Zziwa et al., 2024). Also, Hassan & Ibrahim (2023) averred that by understanding the incident's intent and method, locating the attack's origins, determining who is responsible, and refining future response plans are all made easier by this intelligence. Through spotting anomalies based on behavior, behavioral analytics also helps to preserve privacy while maintaining high security. Defenses against cyberattacks can be strengthened and individual privacy can be responsibly protected by integrating behavioral analytics into security frameworks (Shetty et al., 2024).

In the same vein, Jones et al. (2025) use a hybrid approach to evaluate user profiling in digital forensic investigations, combining case study evaluations with behavioral analysis based on machine learning (e.g., anomaly detection and clustering algorithms). The study shows how AI can effectively spot suspicious patterns, but it also points out drawbacks like possible biases in training data that could result in inaccurate profiling. Furthermore, the study points out that cultural and contextual differences in behavior make it difficult to generalize models across diverse populations. AI-driven forensic applications are made even more difficult by ethical worries about privacy and the possibility of false positives. These restrictions point to the necessity of human supervision and strong validation procedures in order to guarantee trustworthy and equitable research results.

2.1.4 Artificial Intelligence in Identity & Access Management (IAM)

Identity and Access Management (IAM) is being revolutionized by artificial intelligence (AI), which is replacing antiquated static credentials with intelligent, dynamic security solutions (Dunsin et al., 2024). Also, Kaur et al. (2023) opined that insider attacks and credential stuffing are two contemporary threats that traditional IAM systems, which rely on passwords and set rules, cannot withstand. Through behavioral biometrics, AI improves security by identifying distinctive user patterns, like typing style and device usage, to verify identities (Fernando 2023). In addition, it uses risk-based authentication and anomaly detection to instantly identify questionable activity and initiate further verification as necessary. This flexible method preserves smooth access for authorized users while greatly improving security and privacy (Mohammed et al., 2022).

Furthermore, digital forensics' AI-powered Information Assurance Management (IAM) systems keep comprehensive access logs and spot illegal activity, yielding insightful information. They assist investigators in tracking compromised credentials, spotting privilege escalations, and connecting malicious activity to patterns of access (Keshari & Srivastava, 2024). Additionally, Hassan & Ibrahim (2023) stated that AI can spot irregularities and help locate the breach's origin by automating the analysis of authentication data; it expedites forensic investigations and guarantees adherence to privacy laws. In cases involving cybercrime, this enables faster response times and greater legal accountability. However, there are operational and ethical problems with AI in IAM, like possible biases in behavioral profiling or an over-reliance on automated decision-making (Hope, 2024).

Additionally, Olabanji et al. (2024) used a mixed-methods approach in their 2024 study to examine how artificial intelligence (AI) might improve Identity and Access Management (IAM) in cloud environments. In order to determine how elements like hardware/software configurations, computational environments, demographic variables, and technological advancements affect the efficacy of AI-driven IAM systems, the methodology combined multiple regression analysis with a survey of 582 cybersecurity professionals. Improvements in user authentication, authorization, and access control were found to be significantly correlated with these factors. The authors did, however, recognize certain drawbacks, such as possible biases in self-reported data, difficulties extrapolating results across various cloud infrastructures, and the requirement for ongoing AI model updates to keep up with changing security threats.

2.1.5 Artificial Intelligence against Social Engineering & Phishing

The use of artificial intelligence is crucial in the fight against phishing and social engineering, two of the most destructive and successful strategies employed by cybercriminals. These attacks are challenging to identify using traditional security tools because they take advantage of psychological weaknesses rather than technological ones (Kaur et al., 2023). However, Keshari & Srivastava (2024) asserted that AI tackles this problem by examining vast amounts of communication data, including messages, emails, and social media interactions, in order to identify subtle signs of phishing attempts. Furthermore, the study conducted by Priyadharshini et al. (2025) opined that early detection and blocking of fraudulent messages are made possible by natural language processing (NLP), a subfield of artificial intelligence that is able to identify suspicious language patterns, impersonation attempts, and other anomalies that indicate deceptive intent.

Similarly, AI is essential to digital forensics because it improves the post-event analysis of social engineering attacks. It assists in locating compromised accounts, outlining the attack path, and analyzing how the attacker manipulated users or systems (Binhammad et al., 2024). Also, Hope (2024) highlighted that by mimicking phishing scenarios, AI can also be used to test and train users, generating adaptive learning environments that increase staff members' resistance to dishonest tactics. In a world where cybercriminals are always refining their social engineering tactics, this mix of proactive detection and reactive investigation is essential. By lowering human error, which is frequently the cybersecurity weakest point, integrating AI into phishing and social engineering defenses enhances privacy and security (Faqir, 2023).

Furthermore, Schmitt & Flechais (2024) use a mixed-methods approach to examine the role of generative AI in social engineering and phishing. They combine qualitative analysis of AI-generated deceptive content (such as deepfake audio and synthetic text) with simulated phishing experiments. While highlighting limitations like a limited focus on short-term attack scenarios that might not reflect evolving adversarial tactics, the study also reveals AI's alarming efficacy in creating convincing scams. Furthermore, the use of volunteers in controlled trials raises concerns regarding generalizability in the real world. The dual-use risks of publishing detailed methodologies also raise ethical questions. These limitations highlight the necessity of proactive defenses while striking a balance between security and transparency in AI-driven deception research.

2.1.6 AI-Enhanced Encryption and Data Protection

An important advancement in protecting sensitive data from changing cyberthreats is represented by AI-enhanced encryption and data protection (Vignesh Saravanan et al., 2023). However, Mark (2024) stressed that despite their effectiveness, traditional encryption techniques frequently fall behind the complexity of today's data ecosystems and the computational prowess of contemporary attackers. Through real-time vulnerability detection, dynamic key management adjustments, and encryption algorithm optimization, AI tackles these issues (Patil 2024). Although a study conducted by Abbas et al. (2025) highlighted that machine learning models can identify possible breaches or unauthorized decryption attempts by analyzing patterns in data access and usage. This allows for proactive countermeasures. Furthermore, Mohammadiounotiki & Babaeitarkami (2024) opined that data can be processed while still being encrypted due to AI-powered homomorphic encryption, protecting privacy even while analysis is underway.

In addition, AI-enhanced encryption serves two purposes in the field of digital forensics: it protects private information while facilitating investigations. While forensic analysts frequently come across encrypted evidence that can impede or postpone investigations, artificial intelligence (AI) can help detect encryption patterns or possible vulnerabilities without jeopardizing security (Kethireddy 2021). Akhtar et al. (2022) avowed that AI algorithms can expedite legal access to crucial evidence by prioritizing decryption efforts by examining metadata or behavioral hints connected to encrypted files. AI simultaneously maintains stringent privacy controls by guaranteeing that only authorized personnel can access decrypted data (Sharma, 2021). Nevertheless, there are ethical issues with the use of AI in encryption as well, such as the possibility of abuse in producing unbreakable encryption or jeopardizing legitimate surveillance (Kethireddy 2021).

Similarly, Kethireddy (2021) investigates AI-driven encryption methods for cloud data security by using machine learning algorithms to alter encryption protocols in real time according to threat patterns and data sensitivity. The study shows enhanced adaptive security over conventional techniques by combining theoretical analysis with simulation-based testing of AI-enhanced cryptographic models. The computational overhead of real-time AI-based encryption decisions is one of the main drawbacks, which could affect cloud performance for applications that are sensitive to latency. Additionally, the study finds weaknesses in the quality of training data, where incomplete or biased datasets may jeopardize the encryption strategy used by the AI. These limitations point to the necessity of hybrid strategies that strike a balance between established cryptographic standards and AI adaptability in real-world settings.

2.2 Theoretical Framework

This study examines AI-driven cybersecurity by combining the Differential Association Theory (DAT) and Socio-Technical Systems Theory (STS). Dearden et al. (2021) expressed that DAT helps with phishing and social engineering tactic profiling by explaining how cybercriminals learn their behavior through social interactions, while STS ensures strong security design by highlighting the interaction of AI technologies, human factors, and organizational policies

Copyright © The Author, 2025 (www.ijsmr.in)

(Thomas 2024). When combined, these theories offer a prism through which to view the behavioral causes of cyberthreats as well as the structural defenses required to lessen them.

2.2.1 Differential Association Theory (DAT)

Edwin Sutherland developed the Differential Association Theory in 1947 to explain criminal behavior as learned through social interactions and offer important insights into how artificial intelligence (AI) can improve privacy and security (Bhat et al., 2024). Dunsin D. , Ghanem, Ouazzane, & Vassilev (2024) opined that the theory offers important insights into how AI can improve security and privacy in the context of cybercrime and digital forensics. It also establishes that people pick up illegal tactics, motivations, and justifications from the people they associate with. Alam (2021) highlighted that the theory has a direct bearing on how cybercriminals function in online environments.

In addition, the theory aids in the explanation of AI's function in digital forensics by identifying and linking cybercrimes to particular people or organizations. Criminals frequently leave digital fingerprints that mirror the behaviors they have learned from their peers (Faqir, 2023). Jones et al. (2025) expressed that through the analysis of large datasets, AI improves forensic investigations by spotting technical signatures, behavioral patterns, and methods of operation that connect disparate attacks to shared origins. In order to map out the associations between various cybercriminal actors, machine learning algorithms are able to identify minute similarities in malware code, attack vectors, or operational security flaws that human analysts might miss (Akhtar et al., 2022). This ability is especially useful for identifying cross-jurisdictional organized cybercrime networks, where conventional investigative techniques encounter considerable difficulties.

Furthermore, the theory accentuates that AI has the potential to stop the socialization processes that produce new generations of cybercriminals. Aspiring hackers have fewer opportunities to successfully practice and hone their skills because AI automates the detection and neutralization of malicious activities (Jones et al., 2025). Shetty, Choi, & Park (2024) opined that early intervention is made possible by AI-powered predictive policing systems that can recognize people who are at risk of joining cybercriminal networks based on their online associations and digital footprints. AI tools that imitate the methods used by criminals to exploit personal data can proactively detect and fix vulnerabilities in privacy protection before they are turned into weapons (Roshanaei, Khan, & Sylvester, 2024). Bhat et al. (2024) emphasize that the social aspect of criminal behavior is consistent with the dual strategy of disrupting current criminal networks while preventing the emergence of new ones and this shows how AI can drastically change the ecosystem (Jimmy, 2021).

2.2.2 Socio-Technical Systems Theory (STS)

Eric Trist and Ken Bamforth proposed the Socio-Technical Systems Theory (STS) in 1951. through an analysis of the dynamic interplay between technological systems and human factors, it offers a thorough framework for comprehending how Artificial Intelligence (AI) improves privacy and security (Analo 2023). Obidimma & Ishiguzo (2023) expressed that effective security solutions must address both technical vulnerabilities and human behaviors, according to STS, which is relevant to cybercrime and digital forensics. Automating threat detection through sophisticated algorithms that examine network traffic, spot irregularities, and anticipate possible breaches, artificial intelligence (AI) improves privacy and security. In

Copyright © The Author, 2025 (www.ijsmr.in)

addition, it facilitates human decision-making by minimizing human error, speeding up response times, and offering actionable insights. This dual emphasis is consistent with STS principles, which support integrated systems in which technology enhances human knowledge rather than functions independently (Zarei et al., 2024).

Furthermore, AI-driven security solutions' ability to reduce risks across several socio-technical system layers is demonstrated by the application of STS (Abbas et al., 2025). Hope (2024) avowed that, technically, artificial intelligence (AI) improves cybersecurity by using machine learning models that instantly identify and react to threats, like malware or phishing attempts. In order to combat insider threats and social engineering attacks, artificial intelligence (AI) tools such as behavioral analytics track user activity and flag questionable behavior (Faqir, 2023). Also, Dunsin et al. (2024) expressed that AI also helps organizational processes by streamlining workflows, like automating incident response or setting alert priorities for forensic investigators and by ensuring that AI systems respect privacy rights and uphold transparency. STS emphasizes the significance of striking a balance between these technological advancements and ethical considerations.

Similarly, STS emphasizes the necessity of AI systems in digital forensics that are not only technically sound but also socially and legally responsible (Keshari & Srivastava, 2024). Also, Zziwa et al. (2024) expressed that AI speeds up forensic investigations through enormous processing of voluminous data, reconstructing attack timelines, and spotting patterns that human analysts would miss. However, STS highlights that in order to avoid biases, guarantee regulatory compliance, and preserve ethical standards, these tools must be created with human oversight. The theory also points out the value of interdisciplinary cooperation, in which policymakers, legal specialists, and cybersecurity experts collaborate to regulate AI's role in privacy and security (Ezeji 2024).

2.3 Gaps in Literature

Even with increased interest in AI applications, there are still significant knowledge gaps that exist regarding AI's potential to improve security and privacy in the face of growing cybercrime. Different documented research frequently ignores ethical and legal ramifications in favor of technical solutions. Additionally, research on integrating AI in digital forensics is dispersed and lacks a cohesive framework. In order to fully utilize AI's potential in cybersecurity, more thorough, multidisciplinary research is required.

A study on Digital Forensics in Cyber Security: Recent Trends, Threats, and Opportunities was conducted by Alghamdi (2020) and it provides a broad overview of emerging technologies and issues however, the study lacks empirical validation and real-world case studies to support the trends, threats, and opportunities in digital forensics within cybersecurity. It also did not explicitly explicate the practical applications or provide insightful conclusions from forensic analysis. Additionally, the study does not adequately address the increasing legal and ethical complexity of managing digital evidence across jurisdictions, which is crucial for practitioners. The absence of a methodological framework for integrating digital forensics into proactive cyber defense strategies further restricts the study's applicability; this leaves room for future research to fill in these theoretical and practical gaps.

Furthermore, the study by Binhammad et al. (2024) in The Role of AI in Cyber Security: Safeguarding Digital Identity offers a thorough examination of AI's function in cybersecurity, specifically in protecting digital identities. However, it falls short in addressing the adversarial and ethical issues related to AI-driven security systems. The authors go into great detail about AI's potential for threat detection, authentication, and anomaly detection, but they don't go far enough in exploring the ethical ramifications, such as biases in AI algorithms and privacy issues brought on by massive data collection, or the dangers of AI being abused by bad actors, such as through adversarial machine learning or AI-powered cyberattacks. Furthermore, the study's conclusions are not as broadly applicable because it does not provide empirical support for AI-based solutions in large-scale, real-world settings.

In addition, while the study by Abbas et al. (2025) on Leveraging Machine Learning to Strengthen Network Security and Improve Threat Detection in Blockchain for Healthcare Systems provides insight into the use of machine learning (ML) to enhance threat detection and network security in blockchain-based healthcare systems, it ignores the scalability and interoperability issues that arise when integrating ML with blockchain in real-world healthcare settings. The study effectively clarifies how machine learning can identify threats, but it did not thoroughly examine the possible computational overhead, latency issues, and energy consumption associated with deploying ML models on decentralized blockchain networks, particularly in resource-constrained healthcare settings. Additionally, the study lacks empirical validation on a range of healthcare datasets and ignores data privacy and regulatory compliance concerns when combining ML-driven analytics with blockchain's immutable ledger. However, none of this study has examined the role of artificial intelligence in strengthening privacy and security in the era of cybercrime and digital forensics. Therefore, this study aims to examine the role of artificial intelligence in strengthening privacy and security in the era of cybercrime and digital forensics.

3. Methodology

3.1 Research Design

This study adopts a quantitative, exploratory design utilizing secondary data analysis to evaluate the effectiveness of artificial intelligence (AI) techniques, particularly Random Forest Classifier (RFC) and Gradient Boosting Classifier (GBC), in enhancing cybersecurity and privacy within digital forensic frameworks. The focus is on evaluating how well these ensemble models detect and respond to cyber threats using pre-existing cybersecurity datasets that simulate real-world attack vectors.

3.2.0 Data Source and Description

The study relies exclusively on publicly available secondary datasets that are widely used in cybersecurity research and AI-driven threat detection. These include the CICIDS 2017 Dataset, which includes up-to-date intrusion scenarios and normal behavior captured from real-world network traffic.

These datasets provide comprehensive features such as packet duration, protocol types, flag types, service conditions, and intrusion labels. All data are preprocessed to ensure uniform formatting, removal of missing values, normalization of continuous variables, and one-hot encoding for categorical variables where necessary.

3.3 Machine Learning Techniques

Two ensemble learning methods were employed:

Copyright © The Author, 2025 (www.ijsmr.in)

Random Forest Classifier (RFC): A bagging technique that constructs a multitude of decision trees during training and outputs the mode of the classes for classification tasks. RFC is robust against overfitting and performs well on high-dimensional data with imbalanced class distributions. Gradient Boosting Classifier (GBC): A boosting technique that builds an additive model in a forward stage-wise fashion, allowing the optimization of arbitrary differentiable loss functions. GBC is suitable for capturing complex interactions and delivering high prediction accuracy. Both models are trained and validated using an 80/20 train-test split, with performance evaluated through cross-validation (k=5) to ensure robustness.

3.4 Evaluation Metrics

Model performance is assessed using standard classification metrics relevant to cybersecurity:

- Accuracy – Overall correctness of predictions.
- Precision – Ability to identify only relevant instances (low false positives).
- Recall – Ability to capture all relevant cases (low false negatives).
- F1-Score – Harmonic mean of precision and recall.
- ROC-AUC – Evaluates model discrimination capability across all classification thresholds.

These metrics are crucial for measuring threat detection systems, where the cost of false negatives can be particularly damaging.

3.5 Ethical Considerations

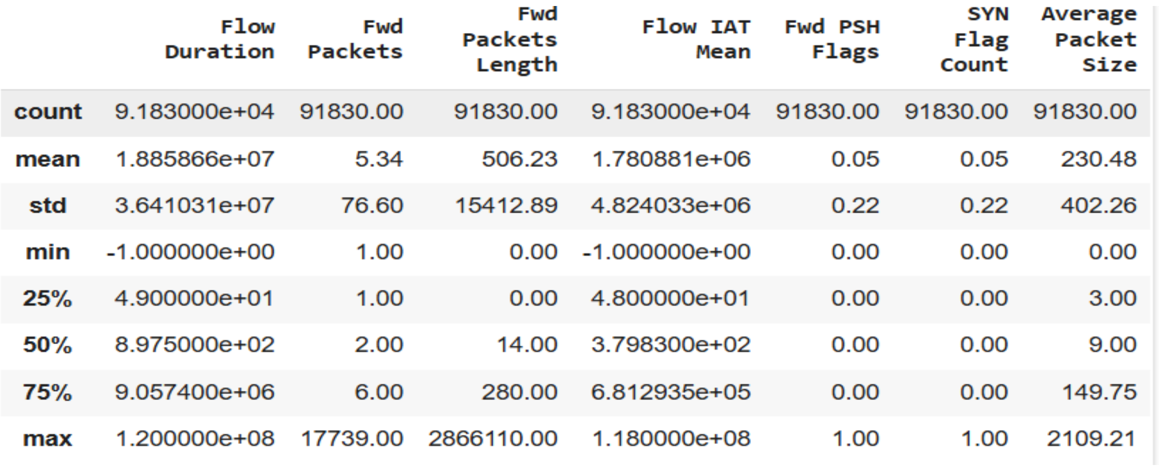
As this study employs only public and anonymized secondary data, it is exempt from institutional ethical approval. However, due diligence is observed in handling the datasets in accordance with privacy and cybersecurity research standards, ensuring that model outputs do not inadvertently disclose sensitive information.

4. Result

Presented in Table 1 below is the descriptive analysis of the features. Flow Duration has a mean of approximately 18.86 million and a standard deviation of 36.41 million, with a minimum value of -1 and a maximum of 120 million, suggesting potential outliers or data quality issues. Fwd Packets has a mean of 5.34 and a max value of 17,739, with a standard deviation of 76.60, indicating high variability. Fwd Packet Length ranges from 0 to 2.86 million, with a mean of 506.23, and Flow IAT Mean has a mean of about 1.78 million and a large standard deviation of 4.82 million, reflecting high variability. The SYN Flag Count and Fwd PSH Flags have values concentrated near zero, suggesting they may not be significant in this dataset. Average Packet Size has a mean of 230.48, with a wide range between 0 and 2,109.21, indicating that some traffic might be disproportionately large. This summary suggests a need for further data cleaning, particularly for outliers in Flow Duration and Flow IAT Mean.

Table 1: Descriptive Analysis of the Features

Copyright © The Author, 2025 (www.ijsmr.in)



	Flow Duration	Fwd Packets	Fwd Packets Length	Flow IAT Mean	Fwd PSH Flags	SYN Flag Count	Average Packet Size
count	9.183000e+04	91830.00	91830.00	9.183000e+04	91830.00	91830.00	91830.00
mean	1.885866e+07	5.34	506.23	1.780881e+06	0.05	0.05	230.48
std	3.641031e+07	76.60	15412.89	4.824033e+06	0.22	0.22	402.26
min	-1.000000e+00	1.00	0.00	-1.000000e+00	0.00	0.00	0.00
25%	4.900000e+01	1.00	0.00	4.800000e+01	0.00	0.00	3.00
50%	8.975000e+02	2.00	14.00	3.798300e+02	0.00	0.00	9.00
75%	9.057400e+06	6.00	280.00	6.812935e+05	0.00	0.00	149.75
max	1.200000e+08	17739.00	2866110.00	1.180000e+08	1.00	1.00	2109.21

In Fig. 1, the histograms show the distributions of key features in the dataset. The Flow Duration distribution is highly skewed, with most values clustered around zero, suggesting that the majority of the flows are very short. Similarly, Fwd Packets, Fwd Packets Length, and Flow IAT Mean exhibit significant skewness, with many instances having values near zero, implying that the dataset is dominated by traffic flows with minimal packet counts and inter-arrival times. The Average Packet Size distribution also follows a similar pattern, with most values concentrated near zero and a small number of larger packet sizes. These distributions indicate the presence of outliers and skewed data, which may require handling, such as log transformations or removal of extreme values, to improve model performance.

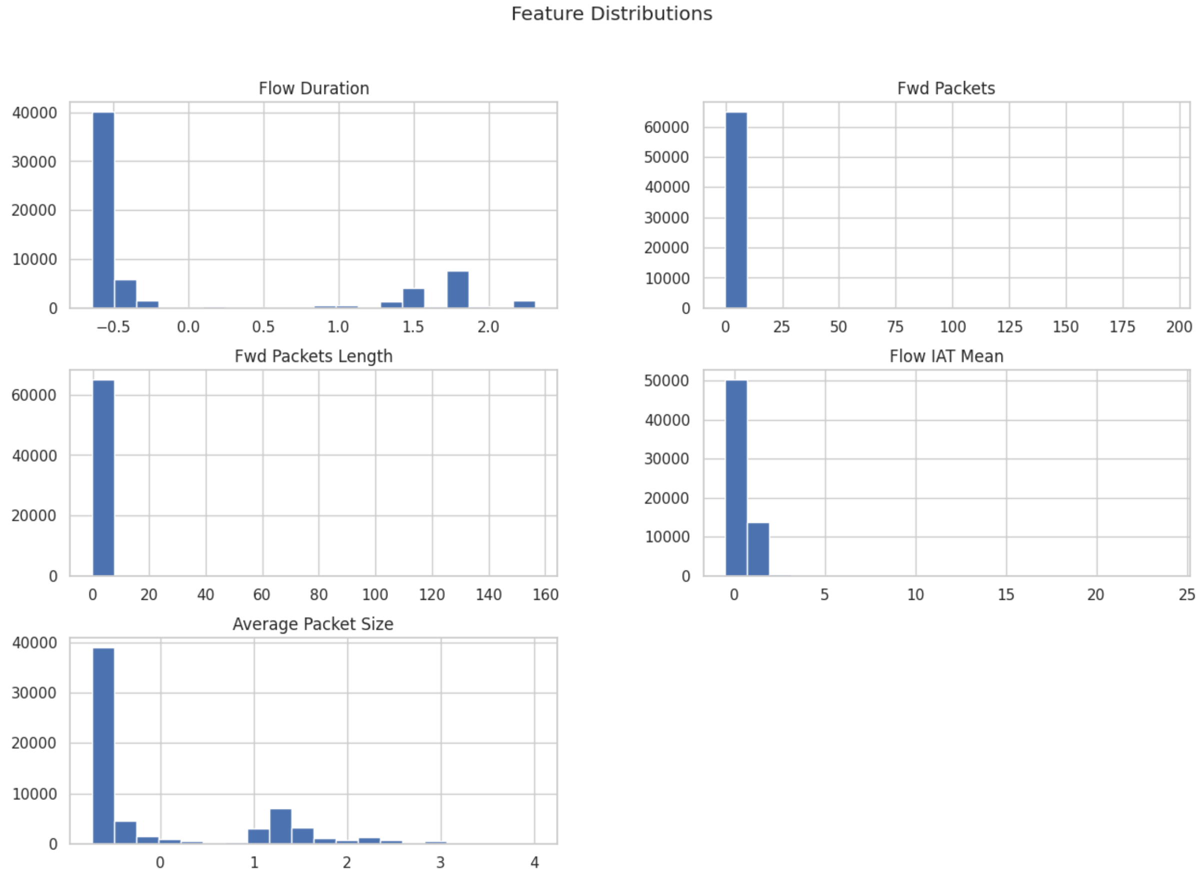


Fig. 1: Histogram Showing Features Distribution

Copyright © The Author, 2025 (www.ijsmr.in)

The bar chart shows the distribution of Normal and Attack labels in the dataset. There is a clear class imbalance, with Attack instances (41,962) significantly outnumbering Normal instances (23,023)

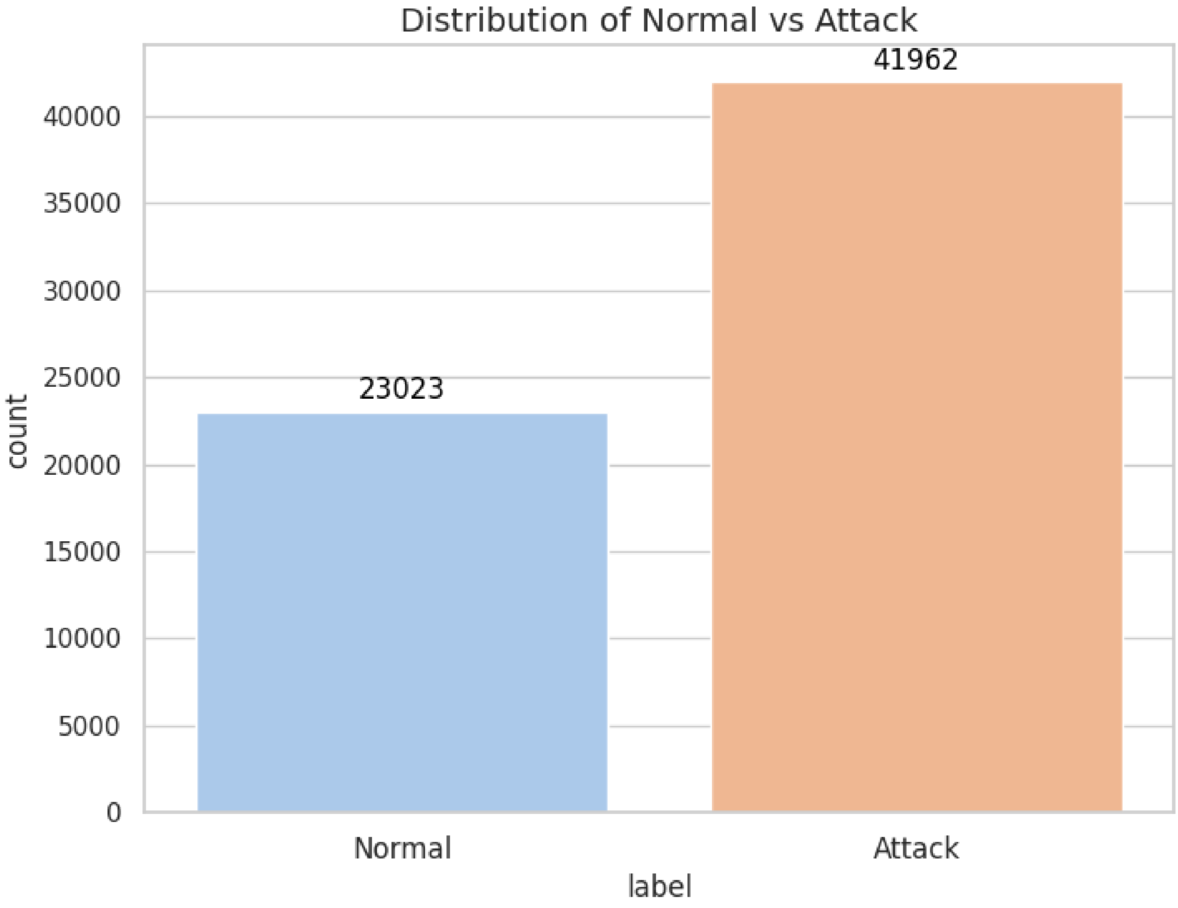


Fig. 2: Bar Chart presenting the distribution of the label

Correlation Matrix

The correlation heatmap indicates that Flow Duration and Flow IAT Mean have a relatively strong positive correlation (r = 0.75), as do Flow Duration and Average Packet Size (r = 0.61). However, no pairs exceed the 0.9 threshold, indicating that multicollinearity is not a major issue in the dataset. Correlations between other features, such as Fwd Packets Length and Flow IAT Mean, are weak, suggesting limited redundancy in the features. This reduces the risk of multicollinearity affecting model performance.

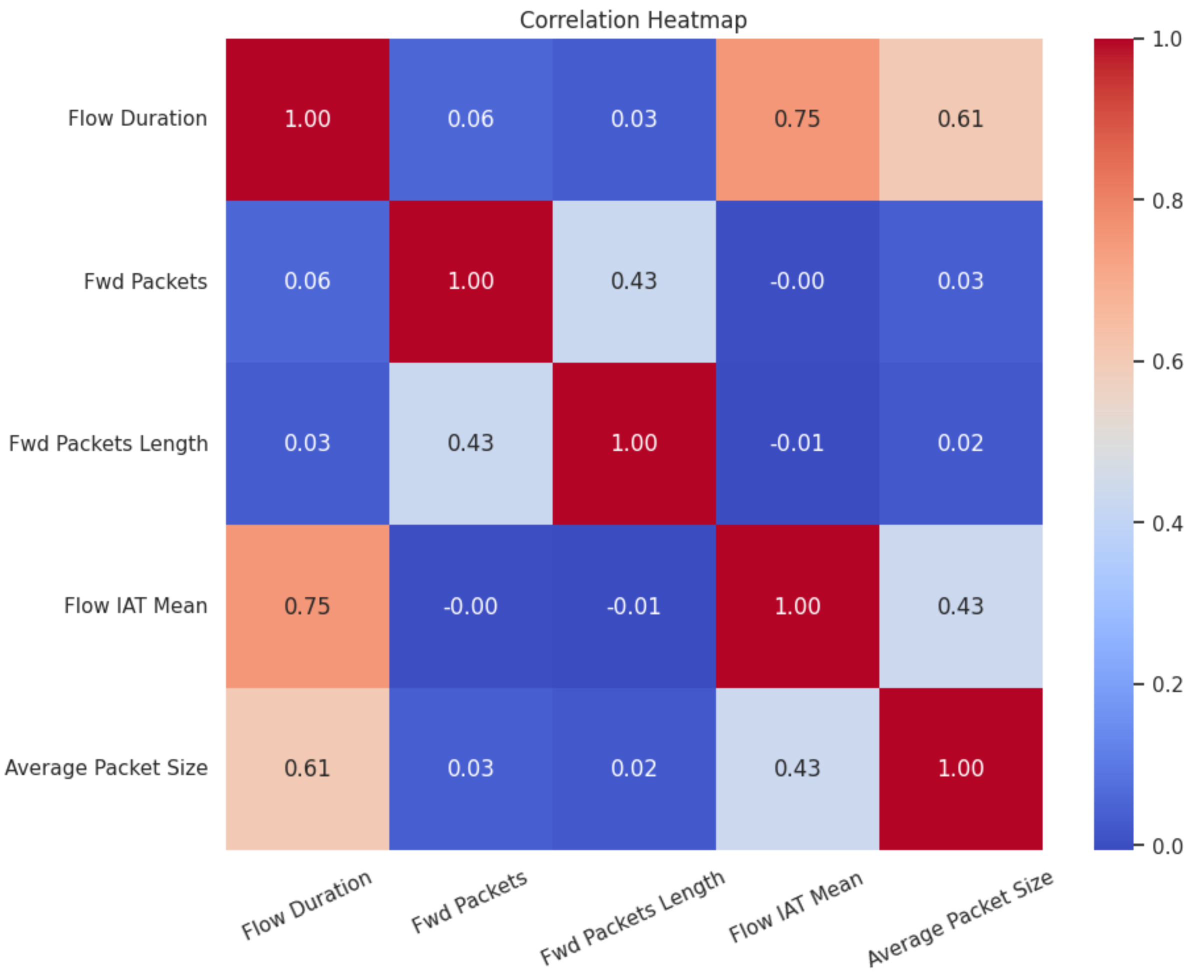


Fig. 3: Heatmap Showing Correlation Analysis.

4.2 Model Performance Evaluation

4.2.1 Hyperparameters

For the Random Forest Classifier (RFC), the optimal model utilized 200 trees (n_estimators = 200), a maximum depth of 20 (max_depth = 20), a minimum samples split of 10 (min_samples_split = 10), and a minimum samples leaf of 2 (min_samples_leaf = 2). These hyperparameters were selected based on five-fold cross-validation, optimizing for the accuracy and F1-score.

For the Gradient Boosting Classifier (GBC), the best-performing model used 200 estimators (n_estimators = 200), a learning rate of 0.1 (learning_rate = 0.1), and a maximum depth of 5 (max_depth = 5). Hyperparameter selection also involved five-fold cross-validation, optimizing for accuracy and F1-score.

Table 2: Best Hyperparameters

Model	**Best Hyperparameters**
Random Forest	n_estimators = 200, max_depth = 20, min_samples_split = 10, min_samples_leaf = 2
Gradient Boosting	n_estimators = 200, learning rate= 0.1, max_depth = 5.

Copyright © The Author, 2025 (www.ijsmr.in)

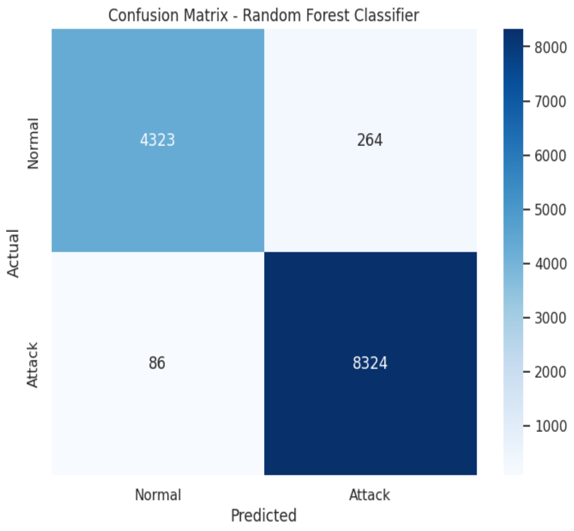
4.2.2 Evaluation Metrics

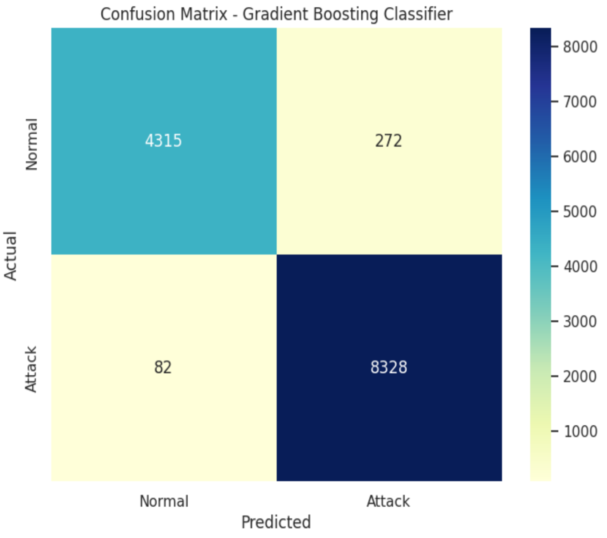
The performance of the Random Forest Classifier and Gradient Boosting Classifier was evaluated using several metrics. The Gradient Boosting Classifier outperformed the Random Forest Classifier in all key metrics. Specifically, GBC achieved an accuracy of 91.3%, higher than RFC's 84.3%. GBC also demonstrated better precision (91.4% vs. 85.9%), recall (91.3% vs. 84.3%), and F1 score (91.2% vs. 83.3%). These results suggest that the Gradient Boosting Classifier provides a more balanced and effective model for distinguishing between Normal and Attack instances.

Table 3: Evaluation Metrics

Metric	Random Forest	Gradient Boosting
Accuracy	0.843	0.913
Precision	0.859	0.914
Recall	0.843	0.913
F1 Score	0.833	0.912

The confusion matrices for both the Random Forest Classifier (RFC) and Gradient Boosting Classifier (GBC) reveal that both models performed well in distinguishing between Normal and Attack instances. For RFC, the model correctly predicted 8,324 attacks (True Positives) and 4,323 normal instances (True Negatives), while misclassifying 264 normal instances as attacks (False Positives) and 86 attacks as normal (False Negatives). GBC showed similar performance with 8,328 true attacks and 4,315 true normal instances, while misclassifying 272 normal instances as attacks and 82 attacks as normal. Although both models demonstrated high accuracy, GBC slightly outperformed RFC, particularly in reducing False Positives and False Negatives, suggesting it may be more reliable in distinguishing between normal and attack traffic.





The ROC curves for both the Random Forest Classifier (RFC) and Gradient Boosting Classifier (GBC) show excellent performance in distinguishing between Normal and Attack instances. Both models have achieved an AUC (Area Under the Curve) of 1.00, indicating perfect classification ability. The curves are sharply rising, suggesting that both models are effectively identifying the positive class (Attack) with minimal False Positives (FPR). These results

Copyright © The Author, 2025 (www.ijsmr.in)

indicate that both RFC and GBC are highly capable of accurately classifying attacks with little to no misclassification

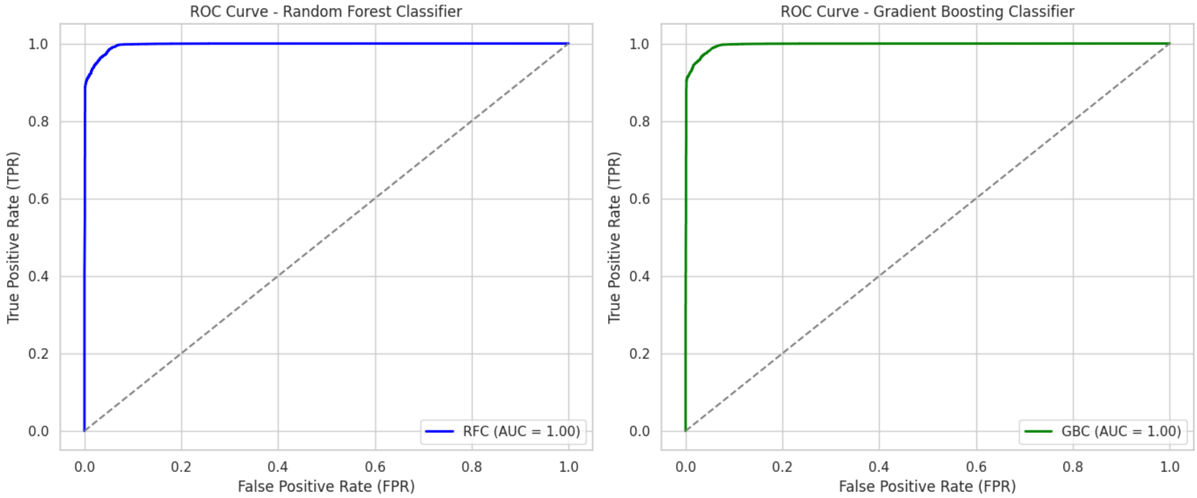
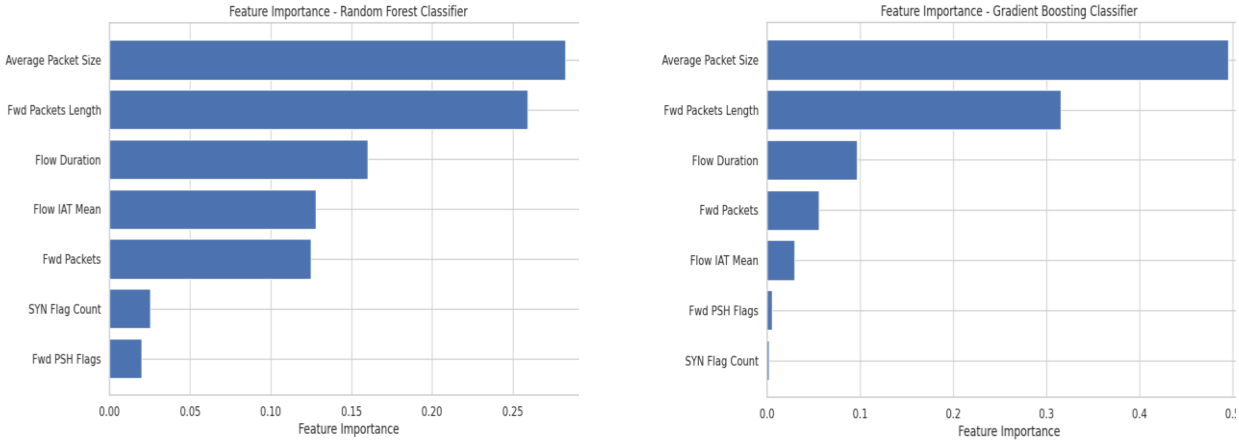


Fig. 5: ROC Curves

The feature importance plots for both the Random Forest Classifier (RFC) and Gradient Boosting Classifier (GBC) reveal that Average Packet Size is the most important feature for distinguishing between Normal and Attack traffic. In both models, Fwd Packets Length and Flow Duration follow as the next most important features, with Fwd Packets and Flow IAT Mean being of relatively lower importance. The features SYN Flag Count and Fwd PSH Flags contribute the least to the model's decision-making. This suggests that packet size and the length of the forwarded packets are more significant indicators of attack detection in this dataset, while flag-related features are less influential. The importance rankings for both models are highly similar, with slight differences in how each model weights certain features.



This study explored the application of machine learning models, specifically Random Forest Classifier (RFC) and Gradient Boosting Classifier (GBC), for detecting cyberattacks based on network traffic data. The analysis revealed key insights regarding both model performance and the significance of different features in distinguishing between Normal and Attack traffic. A clear class imbalance was observed, with Attack instances significantly outnumbering Normal

Copyright © The Author, 2025 (www.ijsmr.in)

instances, similar to challenges identified in previous research on cybersecurity (e.g., Kaur et al., 2023).

Initial descriptive statistics indicated that network traffic patterns were characterized by short Flow Durations and small Fwd Packets, with most flows containing minimal packet sizes. These patterns suggest that legitimate traffic typically involves brief interactions, whereas attack traffic may involve more complex and prolonged data flows. The class imbalance was visually confirmed through a distribution chart, showing the disparity between Normal and Attack traffic. Despite this imbalance, both RFC and GBC demonstrated strong classification abilities, as evidenced by their respective ROC curves, which both achieved an AUC of 1.00, indicating perfect separation between classes.

The performance metrics further differentiated the models. Gradient Boosting Classifier (GBC) outperformed Random Forest Classifier (RFC) in terms of accuracy (91.3% for GBC vs. 84.3% for RFC). GBC also exhibited higher precision (91.4% vs. 85.9%) and recall (91.3% vs. 84.3%), suggesting that it was more effective at correctly identifying Attack instances while maintaining a balance with Normal traffic. On the other hand, RFC demonstrated strong performance but slightly lagged behind GBC in recall, indicating that while RFC performed well in overall accuracy, it may have been less effective in detecting some Attack instances.

The confusion matrices revealed that both models correctly identified a high number of true positives and true negatives, but GBC slightly outperformed RFC in minimizing False Positives and False Negatives, confirming its superior ability to handle class imbalance. The low number of misclassified instances further emphasized the models' effectiveness in distinguishing Attack traffic from Normal.

Feature importance analysis revealed that the most influential features for both models were Average Packet Size and Fwd Packets Length, which were crucial in predicting Attack traffic. These findings align with existing literature, which highlights the significance of packet size and flow characteristics in identifying malicious activities (e.g., Abbas et al., 2025). Less influential features, such as SYN Flag Count and Fwd PSH Flags, had minimal impact on the models' decision-making processes, suggesting that these features may not be as critical in the current dataset.

5.1 Conclusion and Recommendations

This study successfully demonstrated the application of Random Forest Classifier (RFC) and Gradient Boosting Classifier (GBC) in detecting cyberattacks within network traffic data. Both models performed exceptionally well, with GBC achieving higher accuracy, precision, and recall compared to RFC, highlighting its ability to handle class imbalance more effectively. Feature importance analysis identified Average Packet Size and Fwd Packets Length as the most critical features for distinguishing between Normal and Attack traffic, consistent with existing research in cybersecurity. Despite the class imbalance, both models exhibited strong classification abilities, with AUC scores of 1.00 indicating perfect separation between the two classes. The confusion matrices further revealed that GBC outperformed RFC in minimizing False Positives and False Negatives, making it the more reliable model for attack detection. The findings suggest that machine learning techniques, particularly GBC, can significantly enhance cybersecurity systems by providing accurate, real-time detection of network anomalies and malicious activities. Moving forward, class balancing techniques and further hyperparameter tuning could improve performance, especially in detecting minority classes, ensuring a more robust defense against cyber threats.

i. Leverage machine learning algorithms, such as Gradient Boosting Classifier (GBC), to strengthen privacy by detecting anomalies and malicious activities in real-time. These models can monitor and protect sensitive data, ensuring early detection of cyber threats and reducing the risk of unauthorized access to personal information.
ii. To address class imbalance in attack detection, organizations should incorporate resampling or class weighting into their cybersecurity models. This approach ensures that rare, yet critical, attack types are accurately identified, thus improving overall performance in detecting cybercrimes while maintaining privacy and security for users.
iii. Combining machine learning with encryption, secure access controls, and real-time monitoring can significantly enhance privacy. A multi-layered security strategy provides stronger protection against cyberattacks, ensuring sensitive data remains secure even in the face of evolving threats and safeguarding user privacy from cybercriminal exploitation.
iv. Continuous model retraining with updated datasets is essential to keep pace with emerging cyber threats. Regularly adapting machine learning models to new attack strategies ensures that privacy protection measures remain effective and responsive, mitigating risks posed by evolving cybercriminal tactics and maintaining strong defense against privacy breaches.

References

1) Abbas, R., Ogunsanya, V. A., Nwanyim, S. J., Afolabi, R., Kagame, R., Akinsola, A., & Clement, T. (2025). Leveraging Machine Learning to Strengthen Network Security and Improve Threat Detection in Blockchain for Healthcare Systems. International Journal of Scientific and Management Research, 8(2), 147-165. doi: http://doi.org/10.37502/IJSMR.2025.8211
2) Akhtar, M. S., & Feng, T. (2022). Malware analysis and detection using machine learning algorithms. Symmetry.
3) Alam, S. (2021). Adult Delinquency and Victimization: A Test of Differential Association Theory with New Data. West Virginia University.
4) Alghamdi, M. I. (2020). Digital Forensics in Cyber Security—Recent Trends, Threats, and Opportunities. IntechOpen. doi:10.5772/intechopen.94452
5) Ali, A., Septyanto, A. W., Chaudhary, I., Al Hamadi, H., Alzoubi, H. M., & Khan, Z. F. (2022). Applied Artificial Intelligence as Event Horizon Of Cyber Security. International Conference on Business Analytics for Technology and Security (ICBATS), 1-14.
6) Analo, J. (2023). Integration of Artificial Intelligence in Cyber-Physical Systems. Journal of Advanced Technology and Systems, 1(1), 1-12.
7) Bayan, F. M. (2024). The Ethics of AI: navigating the Moral dilemmas of Artificial Intelligence. Arab Journal for Scientific Publishing.
8) Bhat, A. H., & Kolhe, D. (2024). Crime and Fraud at the Community level: Social Networking Understanding into Economic crimes and Psychology Motivations. Journal of Social Sciences and Economics, 3(2), 109-128.

9) Binhammad, M., Alqaydi, S., Othman, A., & Abuljadayeu, L. H. (2024). The Role of AI in Cyber Security: Safeguarding Digital Identity. Journal of Information Security, 15(2), 245-278.

10) Dearden, T. E., & Parti, K. (2021). Cybercrime, differential association, and self-control: Knowledge transmission through online social learning. American Journal of Criminal Justice, 46(6), 935-955.

11) Dunsin, D., Ghanem, M. C., & Ouazzane, K. (2022). The use of artificial intelligence in digital forensics and incident response (DFIR) in a constrained environment.

12) Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. Forensic Science International: Digital Investigation, 48(1), 301675.

13) Ezeji, C. L. (2024). Emerging technologies and cyber-crime: strategies for mitigating cyber-crime and misinformation on social media and cyber systems. . International Journal of Business Ecosystem & Strategy, 6(4), 271-284.

14) Faqir, R. S. (2023). Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview. International Journal of Cyber Criminology, 17(2), 77-94.

15) Fernando, K. (2023). A Multidimensional Framework for Utilizing Big Data Analytics and AI in Strengthening Digital Forensics and Cybersecurity Investigations. International Journal of Cybersecurity Risk Management, Forensics, and Compliance, 7(12), 16-30.

16) Hassan, S. K., & Ibrahim, A. (2023). The role of Artificial Intelligence in Cyber Security and. International Journal for Electronic Crime Investigation, 7(2), 49-72.

17) Hope, C. (2024). Using AI-powered systems to identify and investigate cybercrimes to enhance cybersecurity in law enforcement. Issues in Information Systems, 25(1), 293-304.

18) Iwuh, A. C., & Sonubi, T. (2024). Digital Forensics in Cybercrime Investigation. International Journal of Computer Applications Technology and Research, 13(10), 99-110. doi:10.7753/IJCATR1310.1010

19) Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. Valley International Journal Digital Library, 564-74.

20) Jones, A. J., & Jones, B. M. (2025). Behavioral Analysis and User Profiling in Forensic Investigations. In Digital Forensics in the Age of AI. IGI Global Scientific Publishing.

21) Kaur, R., Gabrijelcic, D., & Klobucar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Journal of Information Fusion, 97, 101804.

22) Keshari, S., & Srivastava, M. (2024). Role of artificial intelligence (Al) in digital forensic vis-à-vis White-collar crimes. International Journal of Law, 10(2), 152-155.

23) Kethireddy, R. R. (2021). Ai-Driven Encryption Techniques for Data Security in Cloud Computing. Journal of Recent Trends in Computer Science and Engineering (Jrtcse), 9(1), 27-38.

24) Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., & Qadir, J. (2023). Privacy-preserving artificial intelligence in healthcare: Techniques and applications. Computers in Biology and Medicine.

Copyright © The Author, 2025 (www.ijsmr.in)

25) Lami, B., Hussein, S. M., Rajamanickam, R., & Emmanuel, G. K. (2024). The role of artificial intelligence (AI) in shaping data privacy. International Journal of Law and Management, 1(7), 2-42. doi: https://doi.org/10.1108/IJLMA-07-2024-0242
26) Madhumitha, P. S. (2024). The Role of Artificial Intelligence in Preventing Cyber Crimes - Indian and International Perspective. Indian Journal of Integrated Research in Law, 4(6), 836-846.
27) Mark, D. (2024). Impact of Artificial Intelligence on Cybersecurity in Nigeria. American Journal of Computing and Engineering, 7(4), 1-11.
28) Matsaung, P., & Masiloane, D. T. (2024). The role of cyber intelligence in policing cybercrime in South Africa: Insights from law enforcement officers. African Security Review, 2(4), 1-16. doi: https://doi.org/10.1080/10246029.2024.2421225
29) Mohammadiounotiki, A., & Babaeitarkami, S. (2024). Cybersecurity in the Age of AI: Protecting Our Data and Privacy in a Digital World. Australian Journal of Engineering Innovative Technology, 6(4), 86-92. doi: https://doi.org/10.34104/ajeit.024.086092
30) Mohammed, R. M., Alneyadi, A., Kassim, N. M., & Yin, T. S. (2022). Conceptual Framework on the Factors Influencing Users' Intention to Adopt AI-Based Cybersecurity Systems at Workplaces in the UAE. Global Business and Management Research: An International Journal, 14(3), 1053-1064.
31) Obidimma, E. O., & Ishiguzo, R. O. (2023). Artificial Intelligence and Cybercrime Investigation in Nigeria: Addressing the Legal and Technical Skills Gaps. African Journal of Criminal Law and Jurisprudence, 13(9), 30-36.
32) Olabanji, S. O., Olaniyi, O. O., Adigwe, C. S., Okunleye, O. J., & Oladoyinbo, T. O. (2024). AI for Identity and Access Management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems. Authorization, and Access Control within Cloud-Based.
33) Patil, D. (2024). Artificial Intelligence in Cybersecurity: Enhancing Threat Detection and Prevention Mechanisms Through Machine Learning and Data Analytics.
34) Priyadharshini, S. L., Abbas, R., Arafat, Y., Batool, W., Abazi, U., & Altemimi, M. A. (2025). Cybersecurity in Al-Driven IT Environments: A Study on Vulnerabilities and Mitigation Strategies. Nanotechnology Perception, 1-19.
35) Roshanaei, M., Khan, M. R., & Sylvester, N. N. (2024). Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions. Journal of Information Security, 15(3), 320-339.
36) Sagar, B., Niranjan, S., Nithin, K., & Sachin, D. (2019). Providing Cyber Security using Artificial Intelligence – A survey. International Conference on Computing Methodologies and Communication (ICCMC), 1-6.
37) Schmitt, M. &. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. Artificial Intelligence Review, 57(12), 1-23.
38) Sharma, S. (2021). Role of Artificial Intelligence in Cyber Security and Security Framework. Artificial Intelligence and Data Mining Approaches in Security Frameworks. doi: https://doi.org/10.1002/9781119760429.ch3
39) Shetty, S., Choi, K. S., & Park, I. (2024). Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Counter measures. International Journal of Cybersecurity Intelligence & Cybercrime, 7(2), 28-53.

40) Singh, U. K., & Bahuguna, R. (2023). The Role of A.I. and Cyber Forensics in Achieving SDG 5 and 16 Dealing in Specific Reference to Cyber Offences Against Women. Dehradun Law Review, 109-120.

41) Stewart, H. (2023). Strengthening Cybersecurity in Digital Transformation. Doctoral dissertation, Flinders University, College of Science and Engineering.).

42) Thomas, A. (2024). Digitally transforming the organization through knowledge management: a socio-technical system (STS) perspective. European Journal of Innovation Management, 27(9), 437-460.

43) Vignesh Saravanan, K., Jothi Thilaga, P., Kavipriya, S., & Vijayalakshmi, K. (2023). Data protection and security enhancement in cyber-physical systems using AI and blockchain. In AI models for blockchain-based intelligent networks in IoT systems: Concepts, Methodologies, tools, and applications. Cham: Springer International Publishing.

44) Yadav, R. T. (2024). AI-Driven Digital Forensics. International Journal of Scientific Research & Engineering Trends, 10(4), 1673-1681.

45) Zarei, E., Biglari, B., & Yazdi, M. (2024). Safety causation analysis in sociotechnical systems. In Safety causation analysis in sociotechnical systems: advanced models and techniques. Switzerland: Cham: Springer Nature .

46) Zziwa, I., Ilolo, A., Nwafor, K. C., & Ihenacho, D. O. (2024). Cloud Computing and AI in Cybersecurity Forensics: Leveraging Data Analytics for Enhanced Threat Detection and Incident Response. International Journal of Research Publication and Reviews, 5(10), 2907-2920.

Copyright © The Author, 2025 (www.ijsmr.in)