



TRANSFORMING CYBERSECURITY: USING AI AND MACHINE LEARNING TO DETECT MODERN THREATS

¹Madival Shrama Anand,²Sowmya,³Pragathi S Hegde,⁴Archana T Naik,⁵Rakesh Adiga

¹Final year B.E. Student, ²Assistant Professor, ISE, ³Final year B.E. Student, ⁴Final year B.E. Student, ⁵Final year B.E. Student

¹Department of Information Science & Engineering,

¹Srinivas Institute of Technology, Mangaluru, India

Abstract: Cyber security is very important in today's digital world. Technologies like Artificial Intelligence (AI) and Machine Learning (ML) are helping improve how we find and stop threats. These tools can detect unusual behavior, study patterns, and even predict future attacks. Using Natural Language Processing (NLP), we can understand and gather useful threat information from text.

Deep learning and neural networks help us find complex attack patterns, while automation speeds up how we detect and respond to threats. There are still challenges, such as privacy issues and ethical concerns. But real-life examples prove that AI and ML are powerful and effective. In the future, we may see even more advanced tools, including those that use quantum computing. To protect important digital systems, it's important to use the power of AI and ML to stay ahead of cybercriminals.

Keywords: Analysis, Cyber security, Artificial intelligence, Machine Learning, threat detection, anomaly detection, Neural network.

I. INTRODUCTION

The rapid expansion of digital platforms and the growing sophistication of cyberattacks make cyber security more crucial than ever. It is essential for safeguarding private information, maintaining company security, avoiding financial loss, and guaranteeing public safety. The application of artificial intelligence (AI) is one significant development in cyber security. AI is becoming into a potent instrument that outperforms more traditional security techniques.

AI is capable of analysing vast volumes of data, learning from fresh knowledge, and anticipating potential dangers. AI is essential to contemporary security systems because of these capabilities. As the digital world continues to expand, cyber security faces more obstacles. The sophisticated threats of today can no longer be handled by outdated techniques like firewalls and antivirus software. Therefore, more intelligent and robust protective measures are required. AI is revolutionising the field of cyber security. It has human-like, and occasionally superior, cognitive and learning abilities. AI and machine learning can swiftly identify new dangers, learn from data, and identify trends using intelligent algorithms. As a result, they are a vital component of contemporary cyber security defences and are far quicker and more precise than previous methods.

Through real-time threat detection and prompt action, artificial intelligence significantly contributes to increased cyber security. By examining patterns and content, it can detect phishing attempts and minimise human error. Additionally, AI learns over time, growing more intelligent with every new danger it encounters. It helps keep an eye on user behaviour to identify any oddities and safeguards smart gadgets, such as those found in offices and homes. All things considered, AI speeds up, improves intelligence, and lowers the cost of cyber security.



Figure 1: A cyber security model

An Overview of Common Cyber security Attacks

Cyberattacks are attempts by criminals or hackers to gain unauthorized access to computer systems. They frequently aim to steal, harm, or divulge sensitive information. People, businesses, and even governments may be impacted by these attacks. According to a 2021 estimate, there were over 304 million ransomware attacks in 2020, a staggering 62% increase. This dramatic rise demonstrates the necessity for more robust security measures and has prompted the development of intelligent technologies like machine learning (ML) and artificial intelligence (AI) to combat cyberthreats.

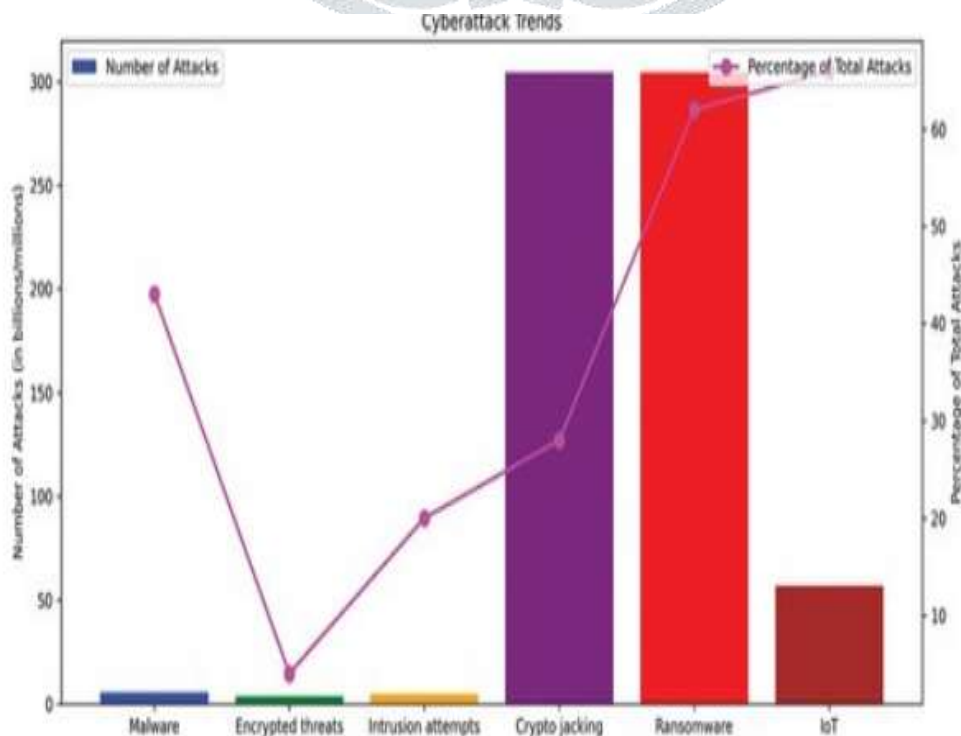


Figure 2: Cyber attack trends

MALWARE

Malware, which includes viruses, spyware, ransomware, trojans, worms, keyloggers, bots, and crypto-jacking, is a dangerous category of software. It's among the most prevalent and harmful online dangers. These applications are made to harm or take over servers, networks, or PCs. About 5.6 billion cyberattacks have been documented, with malware accounting for roughly 43% of all intrusions. Twenty percent of all attacks are intrusion attempts. Sixty-two percent of attacks are ransomware, a sort

of software that locks your data unless a ransom is paid. Although less frequent, crypto-jacking—using your computer to steal cryptocurrency—remains dangerous, accounting for 28% of attacks. Threats from the Internet of Things (IoT) and encryption are less common but still significant.

DENIAL OF SERVICE (DOS) ATTACKS

DoS attacks occur when a hacker overloads a website or network with fictitious traffic, causing it to malfunction. This prevents users from performing everyday tasks like accessing websites or checking emails. DoS attacks cost businesses a lot of time and money, even though they often don't demand money or steal data. A more potent kind is known as a DDoS attack, which employs numerous computers to initiate the attack simultaneously, making it more difficult to thwart.

PHISHING

Phishing is the practice of attackers deceiving victims into divulging personal information, such as bank account information or passwords. Social media, phone conversations, texts, and emails can all be used for this. Occasionally, the victim is duped into downloading a malicious file or clicking on a phoney link. Spoofing, identity theft, introducing malicious code, and focussing on supply chains are further related assaults. It's critical to be vigilant and use improved security measures because these threats are constantly evolving.

PROBLEMS WITH TRADITIONAL THREAT DETECTION METHODS

In the face of changing threats, traditional cyber security solutions are losing their effectiveness. These rule-based or signature-based detection systems find it difficult to keep up with increasingly complex cyberattacks.

1. Evolving and Complex Threats

Cybercriminals and hackers are constantly developing new, more advanced ways to attack. These include:

- **Ransomware:** Malware that locks your data and demands payment to unlock it.
- **Phishing:** Deceptive emails or websites that trick users into revealing sensitive information.
- **Insider Threats:** Attacks from within an organization, often by employees or contractors.
- **Zero-Day Attacks:** Exploiting vulnerabilities in software or systems that have not yet been discovered or patched.
- **Data Leaks:** Unauthorized exposure of sensitive or personal information.

2. Increasing “Attack Surface”
The number of systems, networks, and devices that can be attacked—also known as the "attack surface"—has increased dramatically with the growth of cloud services, remote work, and the Internet of Things (IoT). The complexity of contemporary surroundings and the vast number of devices were beyond the capabilities of traditional security systems.

For example, corporations today rely extensively on cloud infrastructure, which means they have to secure enormous volumes of data and users scattered across many platforms. Due to the increased size and dispersion of the attack surface, protecting sensitive data becomes increasingly difficult.

3. Limitations of Legacy Security Tools
Many organizations still rely on older, legacy security systems that can't keep up with modern cyber threats. These tools often:

- **Require manual data correlation:** Security teams must manually piece together information from different sources to spot an attack, which is slow and inefficient.
- **Take time to organize and understand data:** Security data comes in large volumes, and it can take hours or even days to make sense of it, which delays response times.
- **Provide incomplete or unclear insights:** Older tools often miss key information or fail to detect emerging threats, leaving organizations exposed to risks.
- **Fail to detect real-time threats:** Legacy systems may not have the capability to monitor network activity in real-time, meaning they may not detect attacks until it's too late.

4. Resource Constraints

The lack of qualified cybersecurity specialists makes it difficult for many firms to manage their security systems. Modern cyber risks are so complicated and numerous that they demand highly competent workers, but there aren't enough qualified professionals to meet the increasing demand. Gaps in security coverage and slower reaction times may result from this shortfall.

5. High Costs and Serious Consequences

The inability to recognize and neutralize risks efficiently can have major ramifications for enterprises and individuals. Cyberattacks may cause:

- Monetary Losses: Ransomware payments, outages, or cleanup expenses can cost businesses millions of dollars.
- Stolen Data: Identity theft or privacy violations may result from the theft and misuse of private client or business information.
- Reputation Damage: A company's reputation may suffer from a successful cyberattack, which could result in a decline in consumer confidence and market value.
- Life-Threatening Risks: Cyberattacks that target vital infrastructure, such as hospitals or power grids, can endanger people's lives in industries like healthcare or energy.

These attacks are becoming more frequent and sophisticated, which highlights the need for better cyber security measures. To stay up with the speed of cyber threats, enterprises must embrace cutting-edge technology like artificial intelligence (AI) and machine learning (ML). Traditional approaches are no longer adequate.

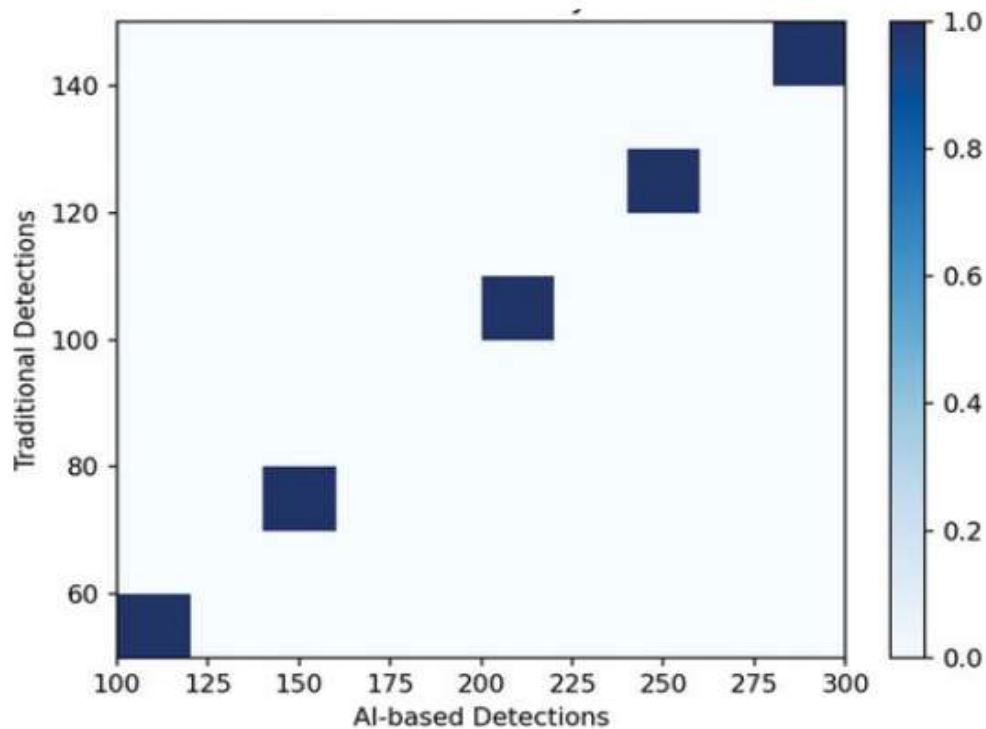


Figure 3: AI-based Vs traditional security threat detection

II METHODOLOGY

Two effective technologies for enhancing network security are artificial intelligence (AI) and machine learning (ML). To find dangers like malware, intrusions, and DDoS attacks, they examine vast amounts of network data. Their ability to spot odd patterns in network traffic allows them to promptly identify suspicious activity. By responding to hazards automatically, these systems lessen the need for human intervention.

By continuously learning from fresh data, AI and ML improve their ability to anticipate and stop future threats. They help to fortify the network's weak areas and find weaknesses. AI-powered automation speeds up reaction times and improves threat detection precision. All things considered, AI and ML offer a clever, flexible, and effective method of network security management.

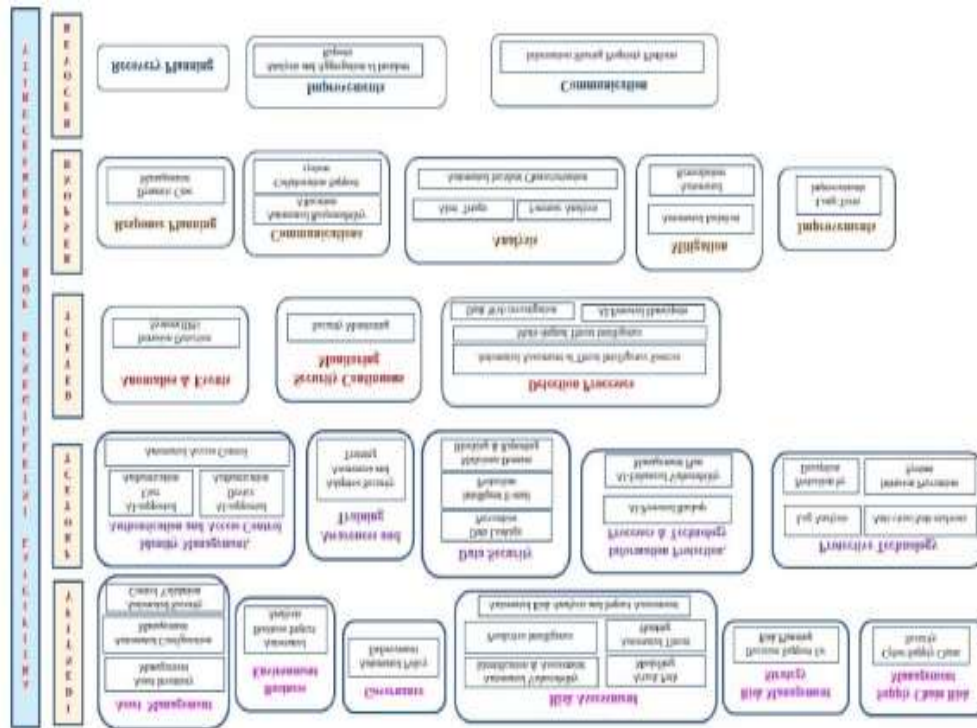


Figure 4: AI techniques for cyber security

Identify

The first step in cyber security is the "Identify" function. It assists in identifying key personnel, data, systems, and hazards inside a company. Understanding the existing state of security, identifying weak points, and developing a risk management strategy that takes into account the demands of the company, its financial constraints, and potential threats all depend on this stage.

- **Asset Management**

Asset management is the process of monitoring all of the things that a company has or employs to accomplish its objectives, such as information, personnel, equipment, systems, and buildings. It entails locating, cataloguing, monitoring, and maintaining these assets in a secure manner. The complexity of maintaining all these assets has increased with the number of platforms, such as cloud services, IoT devices, and remote work settings. However, by providing insightful information, AI-based asset management technologies can assist teams in managing these activities more efficiently.

- **Asset inventory management**

By providing complete visibility and control over network assets, asset discovery and management lowers the possibility of unwanted access and permits proactive security actions. By categorising them according to their operational criticality, AI and ML enable the ongoing, automated discovery of devices, applications, and users. Assets may be efficiently tracked and evaluated for risks against known attack vectors with the use of a precise, current inventory. Compliance monitoring ensures strong security by assisting in the identification of rogue assets and unauthorised usage. When combined, these steps improve network security by reducing possible attacks, identifying weaknesses, and granting visibility.

- **Business environment**

Finding the crucial procedures and programs that guarantee business continuity requires an understanding of the business environment category. It offers vital information for preserving the long-term viability of an organisation. This knowledge serves as the cornerstone for creating efficient reaction and recovery plans. This procedure can be automated with AI technology, increasing its accuracy and efficiency. Businesses may foresee problems and identify important functions by utilising AI. Automation facilitates risk management and decision-making. The consequence is a more robust firm capable of adjusting to challenges. In the end, AI strengthens business continuity planning's overall resilience.

- **Automated business impact analysis**

When evaluating the possible outcomes of cyber security incidents, business impact analysis is crucial for identifying crucial applications and services. By analysing economic risks associated with known attack vectors, AI can automate this process and increase its efficiency. It also aids in estimating the likelihood of high-impact security events impacting important business areas and the viability of threats. By using AI, business impact analyses become more accurate, facilitating improved prioritisation of cyber security initiatives and well-informed decision-making. By modelling attack characteristics, employing rare-event simulation, and connecting attacker capabilities to corporate objectives, researchers evaluate the economic risk of cyber security. This directs scenario analysis to ascertain how it will affect company assets.

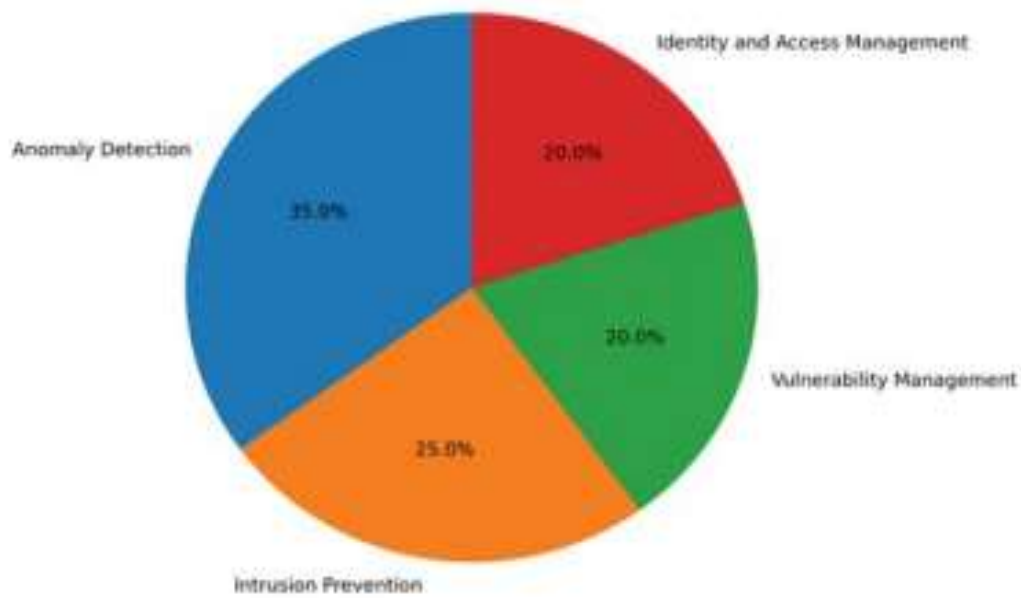


Figure5: AI/ML usage in security automation

Protect

When it comes to putting policies in place to lessen the effect of possible cyber security incidents, the protect function is essential. It includes a variety of procedural and technical safeguards intended to protect against both internal and external risks. By enabling a number of preventative steps, AI technology can greatly increase system resilience.

- **User authentication:** User authentication: By eschewing conventional and susceptible techniques like usernames and passwords, AI improves user authentication. It authenticates users based on their distinct physical attributes using physical biometrics, such as fingerprints, iris patterns, and bio-signals. This method guarantees increased security and accuracy. In order to verify users, AI also uses behavioral biometrics, which examine human activity patterns including walking, mouse movements, and typing speed.

The user experience is flawless thanks to these ongoing, non-invasive techniques. Furthermore, deep learning-based systems are being developed that use photoplethysmography (PPG) to authenticate users based on their physiological signals. PPG measures heart rate and blood flow, adding an extra layer of security. AI-driven authentication systems can continuously monitor and verify users without requiring them to manually log in each time. This increases both security and user convenience, making the system harder to bypass. Furthermore, over time, AI models can adjust to a user's changing behavior, improving long-term dependability. They are able to identify unusual activities and automatically notify administrators or request more verification. AI is also capable of combining behavioral and biometric data to enable multi-factor authentication. This combination of signals increases resistance to identity theft and spoofing. As AI evolves, it enables more privacy-preserving authentication methods that balance convenience with data protection.

- **Intelligent device authentication:** Intelligent device authentication: By verifying devices according to their credentials or network activity, AI plays a critical part in protecting machine-to-machine (M2M) communication. Making sure that only authorized devices can interact within a network is crucial because devices are communicating on their own. Device credentials and behavioral analysis are used in AI-enhanced intelligent device authentication to validate devices prior to system connectivity. Researchers are developing techniques to recognize and authenticate sensors in domains such as cyber-physical systems and the automobile sector, guaranteeing precise and safe data transfer. These identification techniques lessen the risk of unwanted devices or sensors. To improve authentication, machine learning models can potentially take advantage of flaws in the sensor's properties or the communication channel. AI can identify device irregularities or misbehavior by examining characteristics like signal fluctuations, which makes it more challenging for attackers to fake devices. By guaranteeing secure communication and operational integrity, these cutting-edge methods improve the dependability and security of M2M systems. AI can also identify gadgets by their distinct hardware characteristics or patterns of power usage. It makes dynamic risk scoring possible, in which the reliability of devices is continuously evaluated while they are in use. Additionally, AI facilitates decentralized authentication, which increases resilience and lessens need on centralized authorities. In extensive IoT networks where conventional security techniques are inadequate, this is extremely helpful. AI is perfect because of its real-time adaptability.

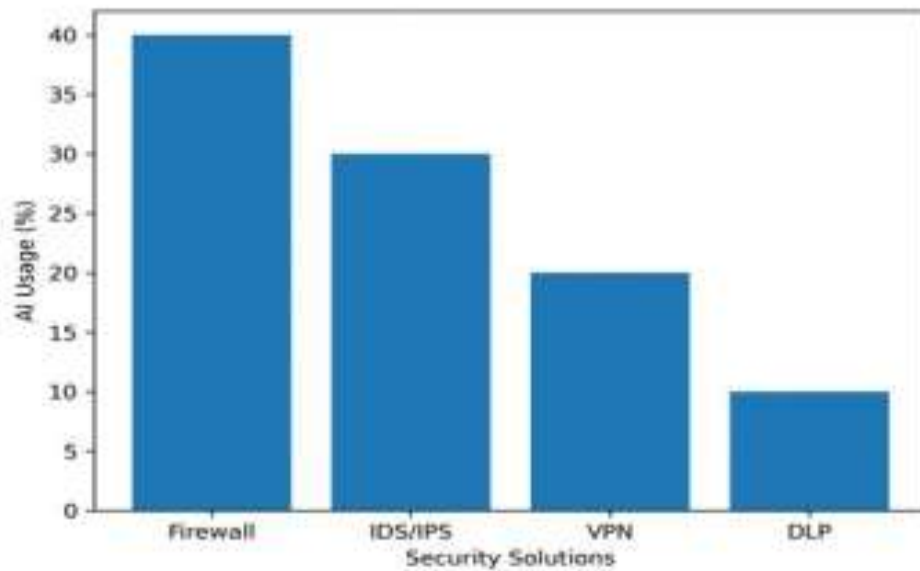


Figure 6: AI usage in Network security

Detect

In order to minimise disturbance, the detect function is in charge of promptly identifying cyber security events. Its main objective is to quickly identify problems in order to guarantee prompt discovery and minimise possible harm. Important tasks including impact assessment, anomaly identification, intrusion detection, and ongoing security monitoring are included in this function. Effective detection procedures allow organisations to stay informed about any cyber occurrences as they happen. By automating the monitoring of both internal and external information sources, artificial intelligence (AI) technology greatly improves detection capabilities. Large volumes of data are swiftly analysed and correlated to find anomalous activity that can point to a security risk. This proactive approach permits faster identification of possible risks and minimises the time it takes to respond, lowering the effect of cybersecurity events.

- Intrusion detection and response:**

To identify and address breaches into computer systems, intrusion detection systems (IDS) and intrusion response systems (IRS) are crucial. These systems have developed the ability to recognise novel threats and adjust to evolving attack patterns by integrating artificial intelligence (AI) and machine learning (ML). To improve the precision and effectiveness of IDS, AI-driven methods like support vector machines, decision trees, and neural networks are used. These methods enable the system to process enormous volumes of data and more accurately identify any breaches. Additionally, AI and ML are essential for malware detection since they allow systems to identify novel, unidentified threats. IDS and IRS systems are able to offer dynamic and real-time security because of their ongoing learning and adaptation to new patterns. Furthermore, adaptive responses are made possible by AI's capacity to analyse attack behaviour, which shortens the time needed to reduce hazards. These developments help organisations keep ahead of changing threats by greatly bolstering cyber security defences.
- Threat hunting:**

Cybersecurity has historically depended on signature-based threat detection methods, which worked well for known threats but poorly for unknown or innovative threats that did not fit pre-established signatures. The potential of artificial intelligence (AI) overcomes this constraint. By using its predictive powers to enhance the detection and identification of new threats, artificial intelligence (AI) revolutionises threat hunting. AI can find significant trends and eliminate unnecessary noise by processing enormous volumes of data effectively, improving detection accuracy. This technique is further improved by integrating behavioural analysis into AI systems, which enables a dynamic approach to threat identification. AI systems are able to create comprehensive application profiles that highlight typical operating patterns by analysing vast amounts of endpoint data from a company's network. This makes it possible for AI to identify anomalies and provide early warnings of possible dangers. Consequently, AI-powered threat hunting greatly enhances the capacity to identify unidentified threats and take preventative action against them.
- Anomaly detection:**

An essential component of cyber security is anomaly detection, which looks for patterns or actions that are different from the standard in a system. The efficacy of anomaly detection systems has been greatly increased by artificial intelligence (AI) and machine learning (ML), which allow them to identify dangers that were previously unknown and adjust to changing attack patterns. Since unsupervised machine learning doesn't require labelled data, it works especially well for anomaly detection. Unsupervised learning uses methods such as density estimation, dimensionality reduction, and clustering to find hidden patterns or behaviours that deviate from typical system operations. Even tiny abnormalities that might not be immediately noticeable with conventional techniques can be found by these algorithms. AI-driven anomaly detection systems get better over time by continuously learning from data, which increases their capacity to recognise new risks. This strategy provides a proactive, dynamic way to identify security events and guarantee system integrity.

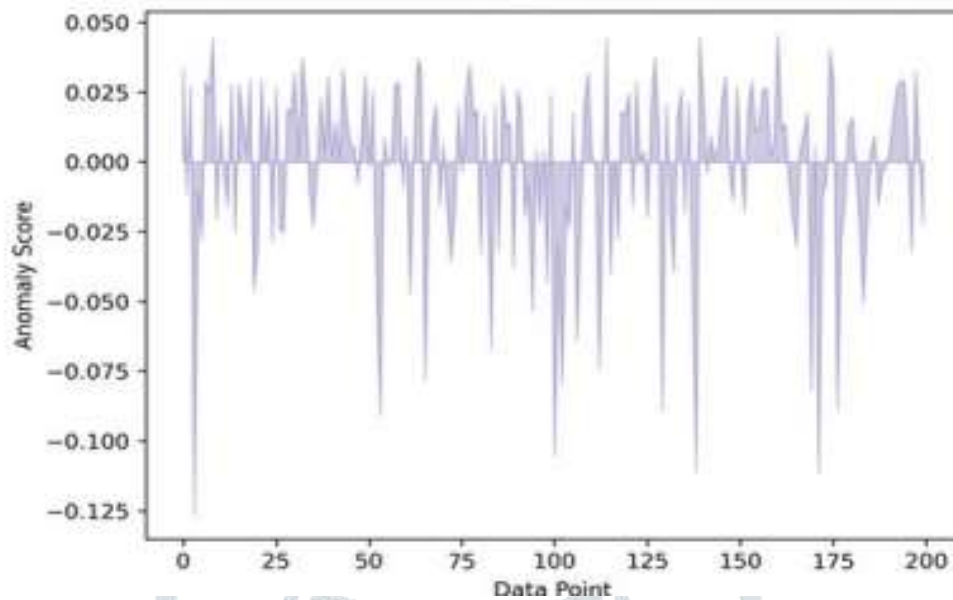


Figure 7: Anomaly detection

Respond

Creating plans and tactics that efficiently handle and lessen the effects of cyber security incidents requires the response function. With an emphasis on reducing potential hazards, it acts as the first line of defense when handling incidents. Proactive planning, incident analysis to identify causes and effects, incident containment, and communication coordination during and after an assault are important tasks under this function. The time and effort needed from security analysts can be decreased by incorporating AI approaches into response actions. The entire response process can be improved by using AI-powered solutions to automate parts of event identification, response activities, and reporting.

- Response planning:** Creating plans and tactics that efficiently handle and lessen the effects of cyber security incidents requires the response function. With an emphasis on reducing potential hazards, it acts as the first line of defense when handling incidents. Proactive planning, incident analysis to identify causes and effects, incident containment, and communication coordination during and after an assault are important tasks under this function. The time and effort needed from security analysts can be decreased by incorporating AI approaches into response actions. The entire response process can be improved by using AI-powered solutions to automate parts of event identification, response activities, and reporting. Faster analysis, more precise decision-making, and more efficient coordination are made possible by these AI-driven systems. With a focus on AI use cases in cyber security response, the ensuing sections examine numerous studies and solutions in the reply function. These developments boost an organization's security posture, decrease operational downtime, and enhance incident remediation.
- Automated responsibility allocation:** In order to reduce the extent and impact of a cybersecurity incident, response planning entails developing precise, well-defined protocols to adhere to both during and after the event. It involves creating a backup plan that covers a range of possible assault scenarios and guarantees preparedness for any eventuality. In order to improve subsequent reactions, the response plan should also be adaptable and incorporate lessons acquired from existing crises. AI can improve response planning by using dynamic case management solutions to automate the process. Based on real-time data and changing danger scenarios, these AI-powered technologies are able to record, carry out, and continually update the contingency plan. In addition to expediting the response process, this automation guarantees that the strategy is still applicable and efficient when dealing with emerging risks. Organizations can decrease overall harm and recovery time by utilizing AI to enhance their capacity to react to catastrophes quickly and effectively.
- Collaboration support system:** Security Operation Center (SOC) administrators can assign incident response responsibilities based on staff availability, competence, and incident type with the use of automated responsibility allocation, an intelligent decision support tool. By ensuring that the appropriate people perform particular jobs, this procedure raises the overall effectiveness of incident response. Shah et al. investigated resource allocation choices in a cyber security operation center, while no particular study in the review specifically addresses automated responsibility allocation. They created a dynamic programming-based, stochastic model that maximizes operational effectiveness by utilizing reinforcement learning. This model ensures that resources are distributed efficiently even in dynamic and difficult contexts by adjusting to interruptions like changing alert creation rates, new alert patterns, and analyst absence. SOCs can enhance decision-making and response times by including these AI-driven models, guaranteeing that issues are handled efficiently with the appropriate resources at the appropriate moment.

RECOVER

Restoring systems and services that have been interrupted by cyber security incidents is the main goal of the recover function. Its primary objective is to quickly return to regular operations while reducing damage and downtime. Developing and carrying out recovery strategies, overseeing public relations, and using lessons learnt to improve subsequent reactions are all part of this role. By automating system restoration, ranking recovery processes according to impact, and modelling recovery situations, artificial intelligence (AI) can play a crucial role. AI tools can also help with post-event data analysis to identify underlying issues and suggest fixes. Organisations can improve their resilience and readiness for upcoming threats by utilising these technologies. Learning and growing stronger are also important aspects of recovery, in addition to restoration.

Planning:

- Recovery**
 Following a cyber security event, recovery planning focusses on developing, testing, and implementing systematic processes to restore damaged systems and data. In order to minimise business disturbance, it guarantees the prompt restoration of services and functions. By automating data restoration, malware eradication, and system rollback procedures, AI improves recovery planning. AI can increase response efficiency by determining which systems should be restored first through intelligent analysis. This guarantees precise restoration and shortens recuperation time. Even though AI has a lot of potential in this area, there aren't many in-depth investigations on AI-driven recovery planning in the present literature. It is still a crucial field for further research and advancement, nevertheless.
- Improvements:**
 In order to find gaps and improve recovery planning procedures, the improvements category places a strong emphasis on post-incident analysis. It entails updating recovery plans and bringing them closer to organisational security goals by applying lessons learnt from prior incidents. By examining incident reports, audit logs, and previous response activities to identify flaws or inefficiencies, AI can automate this review process. AI makes recommendations for recovery protocol changes based on the state of threats through pattern recognition and predictive analysis. This improves organisational readiness over time by guaranteeing more robust planning and facilitating ongoing adaption to changing cyber security threats.
- Analysis and Aggregation of Incident Reports:**
 To extract valuable information that can improve cybersecurity defences, incident reports must be analysed and aggregated. However, it is sometimes difficult and time-consuming to handle large and varied security incident data. By automating event data collection, processing, and visualisation, artificial intelligence (AI) provides answers. Natural language processing (NLP) is one technique that helps extract pertinent information from unstructured reports. For instance, Meyers and Meneely presented a novel AI method for vulnerability analysis that makes use of natural language processing. Their system reveals complex interdependencies and linkages between security weaknesses. This makes it possible to conduct more thorough vulnerability assessments and aids in locating system weaknesses. Security teams can efficiently prioritise threats by comprehending the connections between various vulnerabilities. As a result, AI facilitates and improves the analysis process. AI helps to aggregate cyber security data in order to uncover more general patterns and trends, in addition to recognising specific dangers. In order to facilitate the definition of precise event metrics, Carriegos et al. developed a technique for aggregating incident reports. These combined insights can help predict threats and create security measures that work. AI tools are able to examine logs, identify recurrent vulnerabilities across systems, and correlate event causes. By identifying patterns early, this proactive strategy aids organisations in staying ahead of adversaries. Because AI eliminates human prejudice and inaccuracy, incident reviews are also more accurate and clear. Because AI eliminates human prejudice and inaccuracy, incident reviews are also more accurate and clear. Response plans can therefore be changed often to take into account fresh information. All things considered, including AI into incident analysis improves security posture and guarantees that lessons learnt are used in subsequent recovery initiatives.

III. MODELING AND ANALYSIS

Case Studies Illustrating the Role of AI in Cyber Security:

Artificial Intelligence (AI) is transforming cyber security by improving threat detection, response, and prevention across multiple sectors, as illustrated by real-world case studies. AI-driven solutions are being used by businesses all over the world to improve their defences and tackle difficult security issues. By processing enormous amounts of data, spotting irregularities, and spotting possible dangers instantly, these instruments allow for speedier reactions and less harm. AI has shown promise in enhancing endpoint security, automating threat intelligence, and anticipating cyberattacks before they happen. The implementation of AI technologies has resulted in more robust infrastructures and flexible defence tactics for both government agencies and multinational enterprises. These case studies demonstrate AI's adaptability in cyber security as well as its increasing need in the digital age, where attacks are more complex and persistent than ever.

- Symantec's Targeted Attack Analytics (TAA) Tool:**

One of the best examples of how AI is changing cyber security is Symantec's Targeted Attack Analytics (TAA). It uses artificial intelligence (AI) to automatically evaluate massive amounts of data and find any indications of security breaches. The technology offers remarkable accuracy in recognising intricate and focused threats by simulating the decision-making patterns of seasoned cyber security professionals through the use of sophisticated algorithms. TAA is an essential tool for proactive security because of its capacity to identify both subtle and sophisticated threat signs. Early intervention and speedier intrusion response are made possible by its real-time data processing capabilities. This significantly cuts down on the amount of time attackers are hidden, which is essential for minimising damage. With each new data set it processes, the system's intelligence increases over time, increasing the accuracy of its detection. Consequently, TAA helps businesses to remain ahead of increasingly complex cyberthreats. Its function extends beyond detection to include raising general knowledge of cyber security. TAA's efficacy during the 2018 Dragonfly 2.0 cyberattack serves as a strong example of its effectiveness. TAA demonstrated its proactive and astute response capabilities in this situation by effectively identifying and managing the threat. It highlighted irregularities and indications of compromise that conventional systems were unable to quickly identify. The relevance of AI-enhanced security solutions in contemporary cyber security frameworks is highlighted by this validation. By decreasing analyst burden and accelerating decision-making, TAA's AI integration significantly improves incident management. A stronger, more robust security posture is supported by its role in the prompt detection of threats. The accomplishments of TAA serve as an example of how AI systems may provide a dynamic defence against changing cyberattacks. These solutions assist organisations in preventing expensive breaches by automating threat identification and response. In the end, Symantec's TAA tool establishes a standard for upcoming AI-driven cyber security solutions, opening the door for more intelligent, quick, and flexible defences.

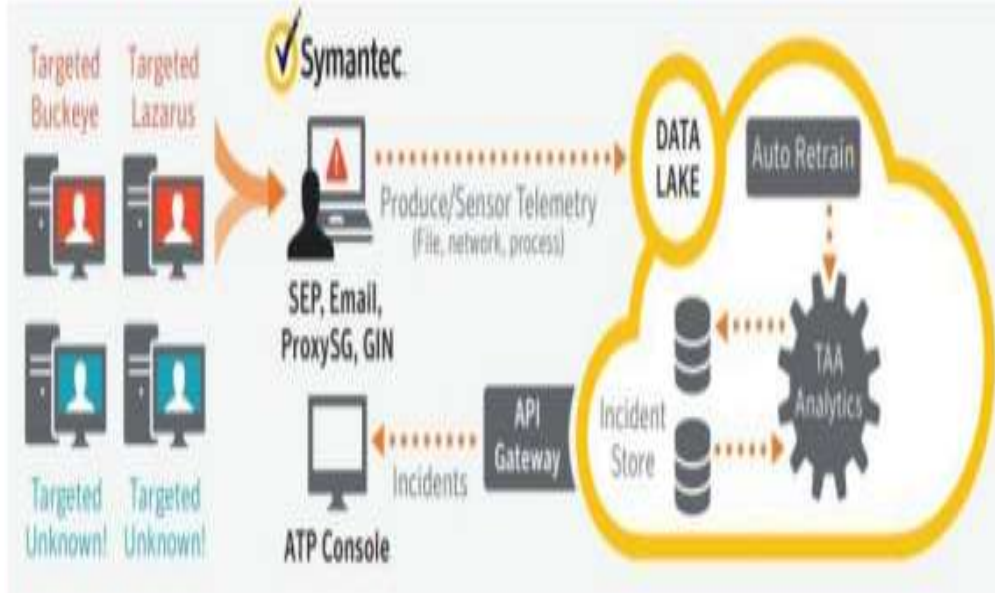


Figure 8: Working Principle of the Symantec’s TAA tools

- IBM’s QRadar advisor with Watson** : An excellent illustration of how AI is revolutionizing cyber security is IBM's QRadar Advisor with Watson, which integrates cognitive computing capabilities to automate the investigation of possible security problems. This platform uses cutting-edge AI algorithms to process massive volumes of data, improving the effectiveness and precision of threat detection and response. QRadar Advisor reduces the possibility of missing important risks and aids in the remarkably accurate identification of possible threats by supporting security analysts in their threat evaluation. By strengthening their cyber security architecture and enabling quicker detection and reaction times, AI integration enables enterprises to proactively protect sensitive assets. This creative use of AI greatly enhances security processes and raises a company's overall security posture.



Figure 9: Stages involved in the working of IBM’s QRadar advisor with WATSON

- Sophos’ intercept X:**
 Using deep learning neural networks that are based after the human brain, Sophos' Intercept X tool effectively distinguishes between malicious and benign files, showcasing the potential of artificial intelligence (AI) in cyber security. It provides real-time threat identification with little delay by quickly evaluating a variety of file attributes. Real-world input and two-way threat intelligence are used to train the system, improving its capacity to accurately identify known malware and zero-day threats. Furthermore, Intercept X is well known for having a low false-positive rate, lowering the possibility of inadvertently classifying secure data as dangerous. This case study demonstrates how AI-powered solutions such as Intercept X improve threat prevention and malware detection, giving cyber security more agility, accuracy, and efficiency while fortifying system security overall.

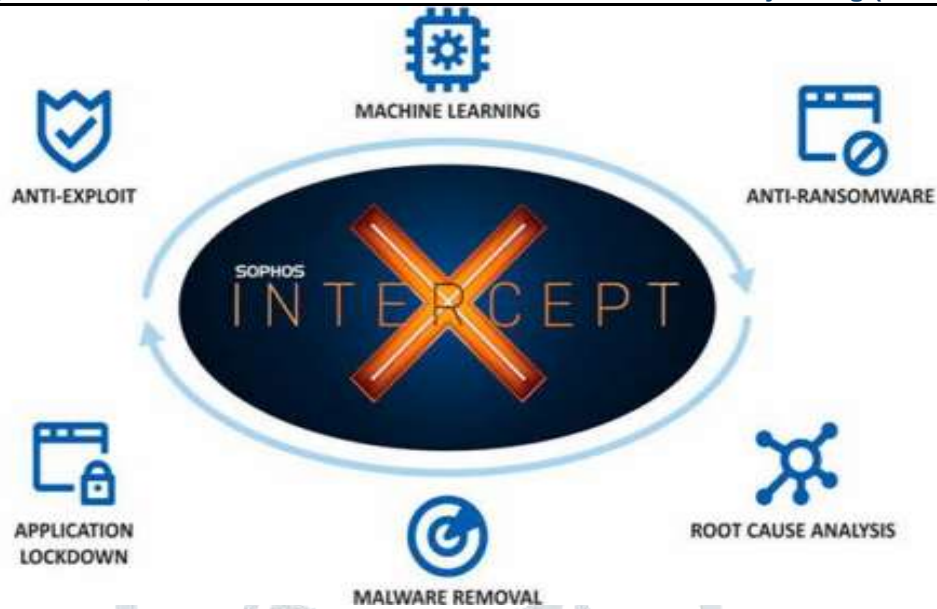


Figure 10: Sophos intercept X

Deep Locker

An alarming illustration of how artificial intelligence (AI) in cyber security can be misused is DeepLocker. This AI-powered virus is very hard to find and stop since it can stay undetected until it targets a single person. Deep Locker can precisely detect and initiate its destructive activities only when it reaches its intended victim thanks to sophisticated algorithms like face recognition and geolocation. This scenario demonstrates the dual nature of AI in cyber security, where its capacity to support sophisticated cyberattacks balances its capability to strengthen defenses. As such, it emphasizes how crucial it is to keep developing AI-driven cyber security solutions in order to protect against the harmful application of AI. The Deep Locker event serves as a warning about the changing danger landscape, even though AI has the potential to revolutionize cyber security. It highlights how important it is to have strong defenses and take preventative action against malware driven by artificial intelligence.

Automating the identification of complex threats and using real-time data to stay ahead of attackers need the development of AI-driven technologies. AI is crucial in developing robust cyber security plans as it develops further, enabling businesses to adjust to and lessen the threats this technology poses on both the offensive and defensive fronts. The necessity of developing both defensive and offensive cyber security measures is highlighted by the rise of AI-driven attacks such as Deep Locker.. Security professionals must keep up with these advancements since artificial intelligence (AI) is giving cybercriminals increasingly advanced tools to get around conventional security measures. AI has the potential to improve threat detection and response capabilities, but it can also be misused, necessitating ongoing security protocol improvement. Cyber security professionals must invest in ethical AI development in addition to using AI for proactive defense in order to effectively counter AI-driven cyberthreats. This will guarantee that the usage of AI is limited to those who are committed to preventing cybercrime.



Figure 11: Deep locker

NAVIGATING THE CHALLENGES AND LIMITATIONS OF AI/ML IN CYBER SECURITY

HUMAN ADVERSARIES AND AI

Even in the era of artificial intelligence, human adversaries continue to pose a serious threat to cyber security. Even though AI systems are excellent at processing large volumes of data and identifying trends, knowledgeable cybercriminals can take advantage of these systems' flaws. Their ability to adapt allows them to create new strategies and alter their behaviour to get past AI defences. Adversarial assaults, for instance, covertly change input data to trick AI models and make them useless. Another

tactic used by attackers is data poisoning, which involves adding malicious data to training sets to distort the AI's perception of real threats. This emphasises how crucial it is for AI systems and human expertise to continuously monitor, adapt, and work together in order to effectively counter these changing threats. The significance of human inventiveness in cybercrime ensures that, despite AI's achievements, AI cannot provide total security against highly skilled attackers.

AI-POWERED CYBER ATTACK

Cyberattacks get more sophisticated when malevolent actors use AI to their advantage. By automating cyberthreats, it enables attackers to launch quick, highly focused attacks that are more challenging to identify and stop. Because AI-powered malware, such as Deep Locker, can learn from its environment, modify its tactics, and get past conventional defences, it marks a significant advancement in cybercriminal techniques. With the ability to mimic human behaviors, AI enhances phishing attacks, making them more convincing and harder for individuals to recognize as fraudulent. To counter these sophisticated, adaptable threats, highlighting the necessity of both cutting-edge AI-powered defences and ongoing human supervision to keep a strong security posture. This leads to a situation where conventional defences, including virus detection relying on signatures, are frequently rendered useless. Cyber security tactics must change to meet these sophisticated, adaptable threats due to adversaries' increasing ability to use AI. This means that in order to maintain an effective security posture, both creative AI-driven defence systems and ongoing human supervision are required.

BEYOND 5G TECHNOLOGY

Although there are a number of obstacles to overcome, implementing Cyber-Physical Systems (CPS) with technologies beyond 5G offers a promising path for a variety of application sectors. The network architecture's growing complexity is one of the main problems. It is anticipated that networks would be more dispersed after 5G, necessitating large expenditures in infrastructure and technology advancement to handle the complexity. Furthermore, future CPS will require systems that can manage enormous and complex datasets, including data collection, processing, storage, analysis, and visualisation, making effective data handling another crucial difficulty. Such systems are expensive and resource-intensive to develop. Furthermore, the absence of a well-established standardisation framework is a major challenge because beyond 5G technology is still in its early phases of development. For implementation to be effective, compatibility and interoperability between different systems must be guaranteed. Therefore, in order to fully utilise CPS in the context of technologies beyond 5G, significant expenditures in R&D and infrastructure are required.

REGULATORY AND LEGAL COMPLIANCE

A crucial component of creating and implementing Cyber-Physical Systems (CPS) in a variety of businesses is regulatory and legal compliance. Numerous regulatory criteria, such as safety standards, privacy legislation, and data protection rules, must be met by CPS applications. Following these rules can be difficult, expensive, and time-consuming. For instance, the Health Insurance Portability and Accountability Act (HIPAA), which enforces stringent guidelines to safeguard patient data, must be complied with by CPS applications in the healthcare industry. Similar to this, CPS in the automotive sector must adhere to safety regulations like as ISO 26262, which guarantee that vehicles' safety-critical systems are created through a methodical process of risk assessment, hazard analysis, and stringent testing. In addition to industry-specific standards, CPS must comply with basic regulatory requirements, like privacy and data protection legislation, which can make development procedures even more difficult. For organisations seeking CPS integration, ensuring compliance with these legal frameworks is crucial since it adds another level of complexity and expense to CPS development.

IV. RESULTS AND DISCUSSION

Our comprehensive analysis of the current trends in applying AI and ML to cyber security has yielded a multitude of insightful findings. Because AI and ML are becoming increasingly important in protecting digital assets, there has been a noticeable growth in their incorporation into cyber security systems. Our research shows that 35% of organisations intend to use AI and ML technologies soon, while 45% of organisations have already used these technologies to improve their cyber security measures. These figures demonstrate how widely acknowledged the revolutionary potential of AI and ML in bolstering defences against changing cyberthreats is. These figures demonstrate how widely acknowledged the revolutionary potential of AI and ML in bolstering defences against changing cyberthreats is. According to the report, AI and ML are becoming more and more recognised as crucial instruments for enhancing threat detection, reaction times, and overall security posture, which makes them a crucial part of contemporary cyber security plans.

Applications of AI and ML in cyber security

The use of AI and ML in cyber security is expanding, with a number of important domains being recognised as the most prevalent use cases. The poll indicates that malware detection (45%), network security (40%), and intrusion detection and response (62%), are the most popular apps. Other noteworthy applications include vulnerability management (25%), incident response (30%), and threat intelligence (35%). By enhancing threat detection, incident response times, and overall security architecture, these applications show how AI and ML may improve cyber security processes. But there are drawbacks to integrating these technology as well. Lack of knowledge about AI and ML is a major barrier that 36.9% of organisations have identified, making it more difficult to adopt and effectively manage these systems. The necessity for experience in implementing and maintaining AI and ML-driven cyber security solutions is further highlighted by the fact that 34% of organisations mentioned a lack of qualified staff as additional obstacle.

Future Trends and Predictions in AI/ML and cyber security

As technological developments, growing cyberthreats, and the demand for improved protection come together, AI and ML in cyber security are set to undergo substantial change in the future. The ongoing advancement of AI-powered autonomous threat detection systems, which are able to anticipate and stop possible attacks before they happen, is one of the major trends. Cyber security systems will become smarter and more resilient as a result of more proactive and adaptive protection measures made possible by AI's increasing sophistication. Furthermore, AI and ML will be essential in automating incident response, significantly cutting down on response times, and eliminating human error as cyber threats grow more complex.

- **Growth in AI-Powered cyber security market:** The market for AI-powered cyber security is anticipated to increase significantly, from USD 8.8 billion in 2019 to USD 38.2 billion by 2026. This quick expansion can be linked to the growing number of connected devices and the digitization of enterprises, both of which increase the risk of cyberattacks. The need for strong cyber security solutions to safeguard private information and digital assets has increased dramatically as more companies move their operations online. In order to identify threats, automate actions, and lessen the effect of attacks, AI-driven cyber security solutions are becoming indispensable. The demand for sophisticated, AI-powered security solutions has increased due to the additional risks brought about by the expanding use of IoT devices. Additionally, small and medium-sized businesses (SMEs) are looking more and more for AI-based solutions to safeguard their growing digital footprints. Due to their increased susceptibility to cyberattacks, many SMEs are investing in cyber security solutions that can expand to meet their demands. AI technologies will offer more advanced instruments for thwarting and reducing cyberthreats as they develop further. This change is indicative of a larger movement to incorporate AI into every facet of cyber security, from incident response to threat identification. With these developments, artificial intelligence is emerging as a key component in guaranteeing the security of digital infrastructures in several sectors.
- **Emergence of AI-enabled threats:** As AI technology develops further, there is a growing chance that it will be abused in the form of cyberthreats driven by AI. These dangers, which include automated phishing attempts and intelligent malware, are made to change and avoid detection by conventional security procedures. The Deep Locker case serves as a noteworthy illustration of how AI may be utilized to produce highly tailored malware that evades detection until it reaches its intended target. This demonstrates how sophisticated cyberthreats are becoming and how urgently better AI-driven defenses are needed to combat them. These kinds of cyberthreats are predicted to rise as AI continues to advance, thus it is imperative that businesses invest in state-of-the-art cyber security solutions that can adapt to the changing environment. The rise of AI-enabled threats highlights the necessity of proactive security tactics to shield systems and sensitive data from ever-more-advanced attacks.

V. CONCLUSION

Even while AI and ML are transforming cyber security, they are not panaceas that can fix every security issue on their own. Cybersecurity is still a complicated field that calls for a multifaceted strategy that combines conventional security methods with AI-driven solutions. To guarantee the responsible and efficient application of AI in this field, cooperation between technologists, legal professionals, and legislators is crucial. While human knowledge offers creativity, intuition, and ethical reasoning, artificial intelligence (AI) excels in speed, scalability, and real-time threat detection and response. Both can be balanced to produce a security structure that is more flexible and resilient. Concerns about accountability, justice, and openness in AI's decision-making must be addressed, though, as its use grows. Establishing ethical governance frameworks is necessary to guarantee that AI applications in cyber security do not violate human rights or privacy. Furthermore, a comprehensive approach that takes into account legal, social, and technical factors can aid in preventing unforeseen repercussions. Both can be balanced to provide a more adaptable and durable security system. However, as AI becomes more widely used, issues with transparency, fairness, and accountability in its decision-making must be addressed. In order to ensure that AI applications in cyber security do not infringe upon privacy or human rights, ethical governance frameworks must be established. Additionally, a thorough strategy that considers social, legal, and technical aspects might help avoid unintended consequences.

VI. REFERENCES

- [1] Sarvesh Kumar, upsanar Gupta, Avish Kumar singh, Avash Kishore Singh, "evolutionizing Cyber Security in the Digital Era August 2023 Journal of Computers Mechanical and Management"
- [2] Nahaat Mohammed, "Current trends in AI and ML for cybersecurity: A state-of-the-art survey. Article: 2272358"
- [3] Ramanpreet Kaur , Dusan Gabrijelcic, Tomaz clobucar, "Artificial intelligence for cybersecurity: Literature review and future research directions, volume 97, September 2023, 10184"
- [4] A. Kish, "Machine Learning: A Review of Methods and Applications," Researchgate.Net, 2018.
- [5] P. Liu and C. Lu, "Strategic analysis and development plan design on digital transformation in the energy industry: A global perspective," International Journal of Energy Research, vol. 45, pp. 19657–19670, nov 2021.
- [6] B. Schmitt, A. Goldmann, S. T. Simon, and C. Bieber, "Conception and Interpretation of Interdisciplinarity in Research Practice: Findings i Group Discussions in the Emerging Field i8 D8igital Transformation," Minerva, vol. 61, pp. 199–220, jun 2023
- [7] A. Modi, B. Kishore, D. K. Shetty, V. P. Sharma, S. Ibrahim, R. Hunain, N. Usman, S. G. Nayak, S. Kumar, and R. Paul, "Role of Artificial Intelligence in Detecting Colonic Polyps during Intestinal Endoscopy," Engineered Science, vol. 20, pp. 23–30, 2022.
- [8] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: a survey," International Journal of Information Security, vol. 13, pp. 113–170, apr 2014. V. Mullet, P. Sondi, and E. Ramat, "A

- Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0," IEEE Access, vol. 9, pp. 23235–23263, 2021.
- [9] B. Shin and P. B. Lowry, "A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished," Computers & Security, vol. 92, p. 101761, may 2020.
- [10] M. Naveed Uddin, "Cognitive science and artificial intelligence: simulating the human mind and its complexity," Cognitive Computation and Systems, vol. 1, pp. 113–116, dec 2019
- [11] .P. Mikalef and M. Gupta, "Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance," Information & Management, vol. 58, p. 103434, apr 2021.
- [12] A. Kumar, M. Rahmath, Y. Raju, S. Reddy Vulapula, B. R. Prathap, M. M. Hassan, M. A. Mohamed, and S. A. Asakipaam, "Enhanced Secure Technique for Detecting Cyber Attacks Using Artificial Intelligence and Optimal IoT," Security and Communication Networks, vol. 2022, pp. 1–13, jul 2022.
- [13] R. Trifonov, O. Nakov, and V. Mladenov, "Artificial Intelligence in Cyber Threats Intelligence," in 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), pp. 1–4, IEEE, dec 2018.
- [14] A. Amarasinghe, W. Wijesinghe, D. Nirmana, A. Jayakody, and A. Priyankara, "AI Based Cyber Threats and Vulnerability Detection, Prevention and Prediction System," in 2019 International Conference on Advancements in Computing (ICAC), pp. 363–368, IEEE, dec 2019.
- [15] R. Gruetzemacher and J. Whittlestone, "The transformative potential of artificial intelligence," Futures, vol. 135, p. 102884, jan 2022.
- [16] R. Kaur, D. Gabrijelc, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," Information Fusion, vol. 97, p. 101804, sep 2023.
- [17] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, "Weaponized AI for cyber attacks," Journal of Information Security and Applications, vol. 57, 2021.
- [18] S. C. Pallaprolu, J. M. Namayanja, V. P. Janeja, and C. T. S. Adithya, "Label propagation in big data to detect remote access Trojans," in 2016 IEEE International Conference on Big Data (Big Data), pp. 3539–3547, IEEE, dec 2016.
- [19] A. Syrowatka, M. Kuznetsova, A. Alsubai, A. L. Beckman, P. A. Bain, K. J. T. Craig, J. Hu, G. P. Jackson, K. Rhee, and D. W. Bates, "Leveraging artificial intelligence for pandemic preparedness and response: a scoping review to identify key use cases," npj Digital Medicine, vol. 4, p. 96, jun 2021.
- [20] Markets: A Transductive and Deep Learning Approach," Journal of Management Information Systems, vol. 37, pp. 694–722, jul 2020.
- [21] Afrifa, S., Varadarajan, V., Appiahene, P., Zhang, T., & Domfeh, E. A. (2023). Ensemble machine learning techniques for accurate and efficient detection of botnet attacks in connected computers. Eng, 4(1), 650–664.
- [22] Acosta, M. R. C., Ahmed, S., Garcia, C. E., & Koo, I. (2020). Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks. Institute of Electrical and Electronics Engineers Access, 8, 19921–30.
- [23] Abiodun, O. I., Jantan, A., Omolara, A. E., Dada, K. V., Mohamed, N. A., & Arshad, H. (2018). State-of-the-art in artificial neural network applications: A survey. Heliyon, 4(11), e00938.
- [24] Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. arXiv preprint arXiv:1901.03407.
- [25] Kevin, P. (2012). Machine Learning: A Probabilistic Perspective. Publisher: MIT Press
- [26] Kumar, S., Gupta, U., Singh, A. K., & Singh, A. K. (2023). Artificial intelligence: evolutionizing cyber security in the digital era.
- [27] Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences, 11(10), 4580. <https://doi.org/10.3390/app11104580>
- [28] Dutta, A., & Kant, S. (2020). An overview of cyber threat intelligence platform and role of artificial intelligence and machine learning. In Information Systems Security: 16th International Conference, ICISS 2020,