Cyber Security and Applications 2 (2024) 100031

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/

Cyber security: State of the art, challenges and future directions

Wasyihun Sema Admass [a,*], Yirga Yayeh Munaye [b], Abebe Abeshu Diro [c]

[a] Department of Information Technology, Assosa University, Assosa, Ethiopia
[b] Department of Information Technology, Injibara University, Injibara, Ethiopia
[c] Department of Cyber Security, RMIT University, Melbourne, Australia

ARTICLE INFO

Keywords:
Cyber-security
State-of-the-art
Challenges
Trends
Future directions

ABSTRACT

Cyber security has become a very critical concern that needs the attention of researchers, academicians, and organizations to confidentially ensure the protection and security of information systems. Due to the increasing demand for digitalization, every individual and organization faces continually shifting cyber threats. This article provides an overview of the state of the art in cyber security, challenges, and tactics, current conditions, and global trends of cyber security. To stay ahead of the curve in cyber security, we conducted a systematic review to uncover the latest trends, challenges, and state-of-the-art in cyber security. Moreover, we address the future direction of cyber security, presenting the possible strategies and approaches to addressing the increasing cyber security threat landscapes, the emerging trends, and innovations like Artificial Intelligence (AI) and machine learning (ML) to detect and automate cyber threat responses. Additionally, this article underlines the importance of ongoing adoption along with collaboration among stakeholders in the cyber ecosystem.

1. Introduction

Indeed, the internet has undergone explosive growth over the past few decades, fundamentally transforming society, the economy, and critical infrastructure. This digital revolution, often referred to as the "cyber civilization," has revolutionized the way we communicate, conduct business, and access information. The speed and scale of this transformation have made the Internet an indispensable source for information exchange and a cornerstone of modern life [1]. People and organizations use technology for business-critical tasks such as banking, health sectors, governments, educational sectors, human resources management, smart cities, and grid systems.

Advances in information and communication technology and the need for quick access to information have made these tasks more convenient to perform and pose serious security challenges that must be addressed by all stakeholders, from individuals to governments [2]. Due to the advancement of technology security issues may be a risk to individuals, societies, and organizations. To mitigate these security challenges, individuals, organizations, and societies often employ various measures, including cybersecurity measures, legal frameworks, and education and awareness campaigns to promote ethical behavior and discourage malicious intent. Cybersecurity is the protection of individuals, societies, organizations, systems, and technologies from abnormal activity. Cybersecurity is the maintenance of the confidentiality, integrity, and availability (CIA) of computer resources owned by one organization or connected to another organization's network [3].

In a world where over 61 % of the industry and social interactions occur online, ensuring high-security standards is essential to facilitate seamless, efficient, and secure interactions some of the key concepts to be considered in ensuring high-security standards is data protection, privacy concern, reliability and availability, and cyber security [4]. Cybersecurity has therefore become the number one means of preventing cybercrime and cyber-attacks by maintaining safe inter-industry and social interactions [5].

Making the internet safer and protecting internet clients has become one of the most critical security issues worldwide [6]. As the digital landscape continues to expand and integrate with almost every aspect of our lives, ensuring a secure online environment has far-reaching implications for individuals, businesses, and nations to improve cyber security [7]. Internet security has become an integral part of the development of new technologies, services, and government policies. Fighting cybercrime requires a comprehensive and safer approach. This means that cybercrime does not occur with technical measures alone. It is critically important that law enforcement agencies can effectively investigate and prosecute cybercrime [8]. Many countries, including Ethiopia, now have strict cybersecurity laws to prevent information leaks.

Peer review under responsibility of KeAi Communications Co., Ltd.
* Corresponding author.
E-mail address: bywasyihun@gmail.com (W.S. Admass).

https://doi.org/10.1016/j.csa.2023.100031
Received 9 July 2023; Received in revised form 25 September 2023; Accepted 1 October 2023
Available online 1 October 2023

Cybersecurity is crucial in the modern digital world because nearly every part of our lives relies on technology to maintain social and economic stability and security. Cyber-attacks can have catastrophic effects, such as financial loss, reputational harm, and even fatalities in industries with vital infrastructure, like healthcare and energy [9]. Cyber security is used in small enterprises, government agencies, military groups, health care providers, educational institutions, energy suppliers, and transportation systems to protect personal data, secure vital infrastructures, and guarantee the confidentiality and integrity of sensitive information [10].

Artificial intelligence (AI) and machine learning can be used for detecting threats, uncovering network vulnerabilities, and reducing IT workloads [11]. In addition, machine learning and artificial intelligence (AI) can be used to automate many of the tasks involved in cybersecurity, such as intrusion detection, malware analysis, and vulnerability assessment [12]. This can free up security professionals to focus on more strategic tasks. Organizations are turning to Machine Learning (ML) and Artificial Intelligence (AI) as effective tools in their cybersecurity armory to tackle more sophisticated cyber threats. We investigate the enormous influence of ML and AI on cybersecurity and how they are altering cyber defenses [13]. However, there are anti-machine learning (ML) attacks. In this paper, we discuss the challenges of cyber security, and future research direction including AI, machine learning, and other states of the art techniques used to combat cyber security challenges.

This article is organized as Section 1) Introduction to Cyber security, Section 2) Application area of Cyber-security, Section 3) State-of-the-art in Cyber Security, Section 4) Related Work, Section 5) Challenges of Cyber Security, Section 6) Opportunities and future research direction of cyber security, and Section 7) conclusion.

2. Application area of cyber security

Cyber security provides confidentiality, integrity, and reliability services for different areas by providing defense mechanisms, intrusion detection mechanisms, and encryption mechanisms [14]. Since industry and social interaction are highly dependent on the internet, cyber security is mainly applicable in the following areas.

2.1. Cyber security in smart grid

The smart grid is the next generation of power systems, and by merging cutting-edge computing and communication technologies, it is anticipated to increase the efficiency and dependability of future power systems with renewable energy supplies, distributed intelligence, and demand response. With a reduced level of response time delay, the smart grid offers clients speedy and improved services, allowing for the effective implementation of solutions for the energy issue [2]. Cybersecurity is a critical concern for smart grids due to the extensive interconnectivity of electronic devices and communication networks in the power infrastructure. Smart grids, which use digital technology to optimize the generation, distribution, and consumption of electricity, offer numerous benefits such as improved efficiency and reliability [15].

Smart grid technology communication networks are mission-critical networks for information exchange in energy infrastructure. The main cybersecurity goals for the smart grid are trust, integrity, and confidentiality [16]. These goals of cyber security can be achieved by implementing authentication, secure communication protocol, Monitoring the network for suspicious activity, and encryption [5]. Smart grid cybersecurity ensures timely and reliable access to and use of information [2]. To maintain trust, confidentiality, and integrity in the smart grid system cyber security can mitigate the potential dangers and risks such as denial of service (DoS), advanced persistence threat (APTs), and unauthorized access to data. Cybersecurity emphasizes how cyber-attacks against the Smart Grid can have negative effects, including power outages, financial losses, and safety risks to improve the Smart Grid's online security. In addition to adopting cutting-edge authentication and encryption techniques, improving threat intelligence and sharing, conducting routine security assessments and audits, and educating stakeholders on cyber security awareness and best practices are also suggested [1].

2.2. Cyber security in vehicular communication

Cybersecurity plays a critical role in vehicle communication systems and infrastructures that enable vehicle-to-vehicle communication, improving road safety, traffic efficiency, and passenger comfort, securing communication channels between vehicles and infrastructure such as road units or traffic control centers, securing the software and hardware components of the vehicle itself, such as electronic control units (ECUs), sensors and actuators, protect the privacy and personal information of drivers and passengers like Location, Driving Behavior, Health, ensure the continuity and availability of vehicle communication systems, especially in emergencies where the system must prioritize critical communications over other modes of transportation [17]. This includes not only performing regular testing and maintenance of the system but also implementing redundancy and failover mechanisms. Cybersecurity in-vehicle communications are essential to ensure the security, privacy, and reliability of the system and to maintain the trust of users and stakeholders. A holistic and proactive approach is therefore required involving all stakeholders in the ecosystem, including automakers, infrastructure providers, service providers, regulators, and users [11].

2.3. Cyber security in smart city

A smart city is an urban area that uses advanced technology and communication infrastructure to improve the quality of life for its citizens. However, the growing reliance on connected systems and devices in smart cities also creates significant cybersecurity risks that must be addressed to ensure the safety and privacy of citizens and the resilience of critical infrastructure. Smart city cybersecurity applications protect critical infrastructure such as power, water, transportation, and communications; protect connected Internet of Things (IoT) devices, including sensors, cameras, and other Internet of things (IoT) devices; ensure citizen's privacy, including the personal information collected, protect disaster recovery systems.

2.4. Cyber security in smart eHealth system

Internet of Things (IoT) -based healthcare applications such as remote patient monitoring, and smart health rely heavily on internet-connected devices to collect health-related data from various sources such as medical devices and mobile apps. The combination of the Internet of Things (IoT) and medical devices will improve the quality of healthcare services, providing continuous medical monitoring and progress reporting on the status of patients requiring real-time preventive intervention. According to the World Economic Forum, more than 10 million records of all kinds were stolen, including social security numbers, patient medical records, HIV test results, and personal information of health care providers. Attacks in this sector have compromised an average of 155,000 records, and that number could be higher, with reports of incidents in which more than 3 million of these medical records in 33 countries were compromised. Cyber security is demanded to safeguard sensitive patient information and defend against cyber threats that can harm individuals and disrupt healthcare services and maintain secure communication between healthcare providers and patients [10,2].

3. State of the art

Cyber security provides a defense mechanism for computing systems, networks, and data against unauthorized access, use, or damage and protects society and the economy from online threats that could jeopardize

the confidentiality, integrity, and availability of various sectors, including business, government, the military, healthcare, education, and energy [14]. This section reviews the current conditions and global trends of cyber security, as well as the existing security measures and tools.

The current cyber security landscape is characterized by the regular emergence of new types of cyber threats and trends which constantly sophisticated and diverse for both individuals and organizations. The most common types of cyber threats in 2022 include malware, phishing attacks, ransomware, social engineering, the threat against data, threat against availability, disinformation and misinformation, supply chain targeting, and distributed denial of service (DDoS) attacks [18]. These cyber-threats can have various impacts on different application areas, such as financial losses, operational disruptions, reputational damages, legal liabilities, physical harm, or even national security risks. The level of digital resilience varies from different industries and regions and in some countries, industries prepare themselves to mitigate and control cyber threats. However, many businesses still struggle to implement effective cybersecurity measures and may remain vulnerable to cyber-attacks. To improve cyber security, companies, and industry uses security technologies and techniques such as intrusion detection and prevention systems, firewalls, antivirus software, and encryption. In addition, businesses are increasingly implementing best practices including frequent software upgrades, strict password guidelines, and employee cyber security training [19].

The global trends and significance of cyber security are being recognized more widely, which has prompted the creation of legal frameworks, international collaboration, and innovation landscapes. To improve cyber security and safeguard people's privacy, industries, governments, educational sectors, and financial services several nations have passed laws and regulations. Guidelines and frameworks have also been created by international organizations like the United Nations and the European Union to advance cyber security and encourage international collaboration [5]. The cyber security landscape is always changing in terms of innovation, with new technology and strategies being created to combat new threats. Blockchain technology is being investigated for safe data storage and sharing, while artificial intelligence and machine learning are being leveraged to improve threat detection and response, cloud computing, and quantum computing are also emerging technologies that offer both opportunities and challenges for cyber security.

4. Related work

The study conducted by [20] provides a comprehensive overview of the use of artificial intelligence (AI) in cybersecurity and discusses the challenges and opportunities of using artificial intelligence (AI) in cybersecurity. The researcher discusses the potential of Artificial intelligence to address cybersecurity challenges and the area of AI for cybersecurity, including the use of artificial intelligence (AI) for anomaly detection, intrusion detection, and malware analysis. It then discusses the challenges and opportunities of using artificial intelligence (AI) in cybersecurity, including the need for big data, the risks of attackers using artificial intelligence (AI), and the need for human oversight. The article concludes with a discussion of the future of AI in cybersecurity and how artificial intelligence (AI) can be used to make cybersecurity more effective.

The researcher [21] Conducted a comprehensive overview of the use of AI in cyber security and discussed the challenges of smart health and cybersecurity, including increasing data volumes and complexity, shortages of skilled professionals, and rising healthcare costs. The researcher examines the potential of artificial intelligence (AI) to address these challenges of cyber security in health care and how to use artificial intelligence (AI) for Smart health and cyber security. The researcher discusses the challenges and opportunities of using artificial intelligence (AI) in smart health and cybersecurity, including the need for big data, the risks of attackers using artificial intelligence (AI), and the need for human oversight.

The study conducted by Gunduz and Das [2] discusses the threats and potential solutions of cyber security on smart grids. The researcher discusses cyber threats such as denial of service (DoS) attacks, malware attacks, phishing attacks, and insider attacks and proposes solutions for cyber security threats the smart grid faces. Some of the potential solutions discussed by the researcher are implementing security measures, and educating employees about cybersecurity threats and solutions.

Zhang et al. [20] researched to detect cyber security threats in Internet of Things (IoT) devices using Deep learning approaches. The researcher discusses the use of deep learning for cyber security threat detection and proposes a combined deep learning approach for detecting pirated and malware-infected files across Internet of Things (IoT) networks and achieving better classification performance with an accuracy of 97.46 %.

Abbas et al. [22] Discuss the valuable contribution of AI in cyber security to prevent, detect, and mitigate cyber threats. The researcher identifies the role, state of the art, and opportunities of using AI in cyber threat mitigation the use of artificial intelligence (AI) in malware detection, Network Intrusion detection systems, Vulnerability scanning, risk assessment, and security automation. The study is conducted based on a comprehensive study to present the use of artificial intelligence (AI) in cyber security to automate tasks, improve decision-making, and detect threats more effectively than traditional methods.

HaddadPajouh et al. [23] also researched the Internet of Things (IoT) threat hunting for malware detection using deep recurrent neural network approaches. The researcher was disappointed with traditional-based malware detection which is no longer effective due to the rapid growth of malware and they propose a deep neural network (DNN) to train the patterns of normal and malicious applications in Internet of Things (IoT) devices. The researcher concludes that the proposed model is more accurate than traditional signature-based methods to detect malware in Internet of Things (IoT) devices. But the author does not consider the impact of evasion techniques which makes the malware more difficult to detect by traditional signature-based methods and it is also difficult to detect by the proposed DRNN models and the approaches need to be evaluated on different Internet of things (IoT) devices.

Liew et al. [24] proposes a novel methodology for analyzing the safety and security of cyber-physical systems by utilizing custom metrics. To ensure a more in-depth safety and security investigation, the researcher proposes an approach that makes use of Systems-Theoretic Process investigation (STPA), a top-down hazard analysis tool, and customized matrices. The researcher wants to solve the limitations of STPA by integrating STPA and Custom metrics. STPA is used to find risky control scenarios that might result in unintended losses. The possibility for these scenarios to be utilized by bad actors is then examined using the custom matrices.

Alshehri [6] conducted research on blockchain-assisted cyber security for the medical Internet of Things (IoT) using artificial intelligence. The researcher discusses the potential of artificial intelligence (AI) and blockchain to improve cyber security in medical IoT. The authors contend that artificial intelligence (AI) used to recognize and stop cyber-attacks by identifying patterns, and blockchain can offer a safe and unhackable mechanism to store and exchange medical data.

Yazdinejad et al. [25] propose an ensemble deep learning model to detect anomalies in the industrial Internet of Things (IIoT) data using learning long-term data relationships, whilst the AE model is used to decrease data dimensionality and highlight key features. To test the model the researcher uses two real-world industry Internet of Things (IoT) datasets. The first dataset was for a gas pipeline, while the second was for water treatment. The model achieved 99.3 % accuracy on the gas pipeline dataset and 99.7 % accuracy on the water treatment dataset.

Mahajan et al. [26] conducted research on the use of blockchain technology to secure cloud-based health data records. The blockchain is an immutable and tamper-proof distributed ledger. This implies that electronic health records (EHRs) recorded on the blockchain cannot be

changed or removed without the permission of all network participants. A smart contract is used to interface the blockchain with the electronic health records (EHR) system. A smart contract is a self-executing contract that is kept on the blockchain. The smart contract is used to limit access to electronic health records (EHRs) and to ensure that electronic health records (EHRs) are only shared with authorized users. The researcher evaluates the proposed model using the real-time electronic health records (EHRs) dataset to achieve a high level of accuracy on the security and safety of electronic health records (EHRs) data on the cloud.

Dykstra et al. [27] researched to investigate the economic benefits organizations could gain from receiving and processing cyber threat intelligence (CTI) supplied by the United States government. The researcher uses a theoretical model to demonstrate how the advantages of receiving CTI are directly related to the difference between the danger level indicated by the CTI and the receiving organization's prior assumption about the threat level. According to the authors' results, government entities shouldn't prioritize providing CTI relating to vulnerabilities with the greatest danger rating. Instead, government agencies should concentrate on disseminating CTI which is most likely to have the biggest impact on businesses that have lower prior views about the danger level.

Lonergan [28] has researched the power of beliefs on US cyber strategies and the researcher employed a qualitative approach to examine the evolution of views about military cyber capability in the United States. They concentrated on a decade of US defense cyber plans, beginning with the 2011 Strategy for Operating in Cyberspace and ending with the 2020 Cybersecurity and Infrastructure Security Agency (CISA) Strategy for Securing the Nation's Critical Infrastructure. The author conducted the research to identify the key themes and gaps in US cyber strategy and compare the thematic area of cyber strategy.

5. Methodology

5.1. Criteria for paper eligibility selection process

This systematic review is conducted based on Preferred Reporting Items for Systematic Reviews and Meta-Analyses statement [29] and the search is conducted from 2013 up to 2023. Due to the large number of papers published in reputable journals, we consider papers published within 10 years. In addition, we consider papers published in peer-reviewed journals written in English. Finally, we only include papers that are related to cyber security, the application of Cyber security, and the Challenges of cyber security.

5.2. Information sources

Using multiple databases is a common and effective approach to ensuring comprehensive coverage of the literature on a specific topic, like cybersecurity. In this case, we have chosen four databases: IEEE Xplore, Scopus, SpringerLink, and Web of Science. This is a good selection, as these databases cover a wide range of academic sources related to your topic.

5.3. Search

When we conduct a literature search across multiple databases, it's essential to develop a systematic search strategy, including relevant keywords, Boolean operators, and inclusion/exclusion criteria. Additionally, consider using reference management tools to organize and manage the articles you find during your search. In this article, we use relevant keyword-searching mechanisms. We collected 200 papers through search keyword (search string) methods.

5.4. Selection process

To manage the large number of search results, we conducted an abstract analysis to determine the relevance of each article. The criterion for relevance was whether the abstract indicated that the article related to cybersecurity. If the abstract mentioned addresses the causes or impacts of cyber risks and measures in the area of cybersecurity, the article passed this initial screening. After initial screening, we reduced the articles from 200 to 40. After we reduced the articles, we conducted a full review. The selected 40 articles were read in their entirety. This comprehensive review allowed for a more in-depth assessment of each article's content.

6. Challenges of cyber security

In the digital era, cyber security is a critical concern for people, corporations, and governments. With the increased use of technology and digital devices, it is more necessary than ever to secure electronic devices, networks, and data against unwanted access, theft, and damage. With the advancement of technology, the cybersecurity action of protecting an organization, employees, and critical assets from cyber threats faces several challenges. In this article, we will discuss the challenges faced by the cybersecurity industry and the future directions that can help address these challenges.

6.1. Sophisticated nature of cyber-attacks

The complex nature of cyber-attacks to gain unauthorized access to computer systems and networks poses a significant challenge in the area of cyber security [30]. Intruders (cyber attackers) develop and employ very sophisticated and advanced techniques to gain unauthorized access or exploit vulnerabilities. Some of the complex cyber-attacks that use more advanced techniques to breach defenses and exploit a vulnerability are multi-vector attacks, Polymorphic and Fileless Malware, zero-day exploits, and advanced persistent attacks [9].

Advanced persistent threats (APT):- are sophisticated, targeted, and organized attack that specifically targets the diplomatic, information technology industry, Military services, chemical industries, and other sensitive areas to filter confidential information and damage the targeted industry or area through maintaining persistence using different ways [31]. The APT is a state-sponsored attack by governments and organized criminal groups to get economic, political, and strategic advantages by stealing information and resources from critical infrastructure and industries such as diplomats, national defense, government institutes, manufacturing industries, military plans, and other sensitive areas [32]. One of the APT attacks was the "Aurora operation" a sophisticated cyber-attack that happened in 2009 that targeted technology companies and IT industries such as Google, Adobe, Juniper Networks, and others. The attack was very complicated and used very advanced techniques to steal intellectual property and break into the networks of the targeted technology companies and organizations [32,31,30].

Zero-day exploits are attacks that target newly discovered vulnerabilities that software developers have not yet addressed. Organizations become susceptible when attackers sell or use these vulnerabilities before they are found or fixed. Advanced threat intelligence, behavior-based analysis, and prompt software patching are necessary for identifying and thwarting zero-day exploits. [33]. The vulnerability attacks of the zero-day exploit have divided their cycle into five stages,

- **Zero-Day Attacks**: These are the initial attacks that exploit vulnerabilities that are not known to the public or the software/hardware vendor. These vulnerabilities are typically discovered by malicious actors (black hat hackers), and they do not disclose them to the public or the affected party. Example: - Stuxnet was a highly sophisticated computer worm that targeted supervisory control and data acquisition (SCADA) systems, particularly those used in Iran's nuclear

facilities [10]. It exploited multiple zero-day vulnerabilities to gain access and manipulate industrial systems, causing physical damage to centrifuges used in uranium enrichment.

- **Pseudo-Zero-Day Attacks**: Pseudo-zero-day attacks occur when the exploit is still relatively unknown, but it may have been discovered by a limited number of attackers. The vulnerability may not be widely publicized, but it's not as closely guarded a secret as in the first stage.
- **Potential for Pseudo-Zero-Day Attack**: At this stage, there may be indications or clues that a vulnerability exists, but it hasn't been widely exploited yet. Security researchers or organizations might suspect the presence of a vulnerability based on unusual or suspicious activities.
- **Potential for Zero-Day Attacks**: In this stage, details about the vulnerability have been made public. This might happen when a security researcher or a responsible disclosure process informs the affected party about the vulnerability, or it might become known through other means. Automated attack code or programs for exploiting the vulnerability may start to appear, making it more accessible to attackers.
- **Passive**: This stage refers to the period after a vulnerability has been discovered, disclosed, and patched by the vendor or mitigated in some way. During this time, the vulnerability is no longer a zero-day, and organizations are expected to apply patches or countermeasures to protect their systems.

Zero-day attacks are indeed challenging to detect because they target vulnerabilities that are unknown to defenders, making them like invisible arrows. Detecting and defending against such attacks often require proactive security measures, intrusion detection systems, and rapid response to newly discovered vulnerabilities once they become known.

6.2. Internet of Things (IoT) security

The Internet of Things (IoT) is an emerging technology that connects billions of computing devices with the Internet. The Internet of Things (IoT) interconnects sensors, and computer devices with Internet protocols to exchange information and share data [2]. The Internet of Things (IoT) presents numerous serious cybersecurity concerns as a result of its vulnerabilities [34].

Device vulnerability Internet of Things (IoT) devices are created with minimal processing power and memory, rendering them vulnerable to security flaws. Weak default configurations, obsolete firmware/software, and a lack of security upgrades can make devices ideal targets for cyber-attacks [34].

Data Privacy in Internet of Things devices captures and communicates massive volumes of sensitive data, including personal information. It is critical to protect the privacy and confidentiality of this information. However, insecure data storage, poor encryption, and incorrect data management methods can all lead to unwanted access and data breaches [9]. Internet of Things (IoT) devices frequently rely on wireless communication protocols such as Wi-Fi, Bluetooth, or cellular networks for network security. Attackers may target these communication routes for eavesdropping, interception, or data modification. Insecure network setups and insufficient encryption can jeopardize Internet of Things (IoT) network security [35].

6.3. AI-driven attack

Cybersecurity challenges have been becoming more complex and challenging due to the rapid growth of technological advancement and increasing digitalization in different domains making cyber security more challenging. One of the advancements of technology is artificial intelligence (AI) and Machine learning and currently emerging trends of cyber-attack is the use of AI and Machine learning technology. Even if Artificial Intelligence (AI) has a positive impact on cyber security, there is also a negative impact which is artificial intelligence (AI) driven attacks. Attacks that use AI technology are two types: 1) Artificial Intelligence (AI) assisted attack which uses Artificial Intelligence (AI) and machine learning technologies or techniques to help human attackers plan or execute cyber-attacks and 2) artificial intelligence (AI) autonomous attack use artificial intelligence (AI) and machine learning technology or Artificial Intelligence (AI) agents to carry out cyber-attacks on various industries autonomously without any human intervention. Some of the threats performed by AI-driven attacks are: -

Deep fake attacks [36] are done through artificially generated false and convincing media that uses AI and Machine learning technology to generate realistic images, video, audio, or text that can trick or impersonate humans or systems during social engineering attacks. Deep fakes can be used for a variety of malicious goals, including disseminating false information, blackmailing, faking biometric authentication, and so on. AI-generated images, video, audio, and texts can be purposively used to fool the AI and machine learning models or systems used for cyber security purposes, to invade and mislead security systems that depend on AI and machine learning systems like AI enable malware detection, spam filtering, facial recognition and other biometric security mechanisms [37].

Botnet attacks [35], botnets are interconnected devices that are centrally controlled by cyber criminals to perform different attacks on the targeted area. Some of the attacks done by botnets are distributed denial of service attacks, spamming, stealing data, and others. The botnet attack uses AI and machine learning technology to patch security vulnerabilities and increase the speed of attack by automating and scaling up the attacks to find targets, coordinate attacks, and evade detection [38].

Reinforcement learning enables the agent to learn from its own experience and action and rewards from the environment. Hence, the RL machine learning technology helps autonomous artificial intelligence-enabled cyber-attacks which adapts, learns, and optimizes the strategies based on their feedback and response from the targeted system and automates the processes of patching and exploiting the vulnerability [13].

AI-driven cyber-attacks is a more complex and sophisticated attack which is challenging to cyber security and society. Since the attacks hide and change their situation, it is difficult to detect and attribute the attacks. AI-driven attacks automate the operation of attacks that scale up at high speeds making the attack unable to defend and damaging the targeted resources.

6.4. Cloud computing

Cloud security adoption and increasing dependence on cloud services introduce new threats and vulnerabilities for organizations. Organizations that depend on cloud services experience cyber security challenges such as data breaches, unauthorized access, insecure API, and shared infrastructures which introduce security risks, data loss, and service disruption which leads to unavailability of critical services and other security threats and challenges by faced the given organization [18].

7. Opportunities, future research directions

Cybersecurity is a dynamic and evolving field that provides academics and innovators with several opportunities and difficulties. Several potential avenues are being investigated to address the difficulties confronting the cybersecurity industries,

Advanced artificial intelligence and Machine learning techniques to develop defensive technologies against cyber threats, improve cyber threat detection, automate cyber security processes, and prevent cyber-attacks. Since the cyber-attack become more complex and sophisticated it needs to automate the cyber defense mechanism by using Artificial intelligence and machine learning technology to enhance cyber security. Real-time AI enables cyber threat detection systems to help the cyber

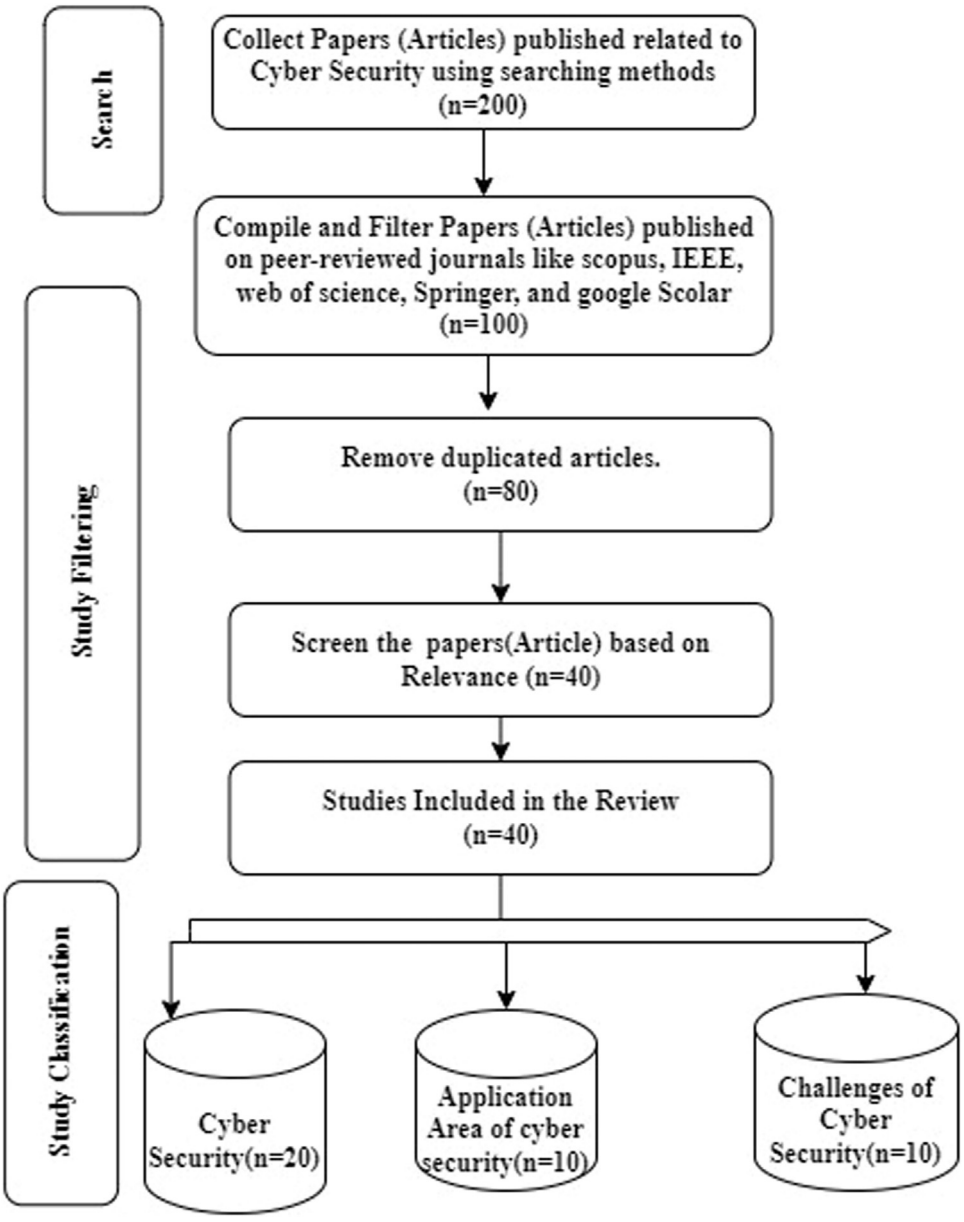

Fig 1. Literature search process and categorization of the studies.

expert analyze the vast amount of data, detect cyber-attack patterns, identify threats and anomalies, and automate security responses to help cyber professionals respond to cyber-attacks more effectively. In addition to artificial intelligence (AI) and machine learning (ML) technology, Biometric Authentication is the most effective technology to secure the targeted industries. Biometric authentication, which validates a user's identification using unique biological features such as fingerprints or facial recognition, can improve security. Biometric authentication, when combined with standard authentication techniques such as passwords, makes it more difficult for thieves to get access to networks and data.

The development of quantum computers was also one of the challenges for the cyber security of existing cryptographic systems and to detect and respond to any attacks related to the development of quantum computer technology, there should be quantum-resistant cryptography technology. Future researchers should focus on quantum-resistant algorithms for cryptography that can withstand quantum computer attacks, ensuring the long-term security of sensitive cryptographic data. The other critical concerns of cyber security challenges are the lack of skilled professionals and people have knowledge gaps about cyber security and its risks. In the future the academician, researcher the government should focus on improving human awareness and education about cyber security (Human-centric security). Understanding the role of human behavior in cyber security should great future focus for academicians, researchers, and governments. Human-centric security includes promoting cyber security best practices using advocacy, developing security user interfaces that are more interactive with users like Chabot applications, and research on socio-technical aspects of cyber security.

The automation of security processes to automate the response to cyber threats is a very crucial point in the cyber industry. The ability of Organizations to respond to attacks can be improved by automating security processes and orchestrating security tools. To automate the security response, there will be a focus on developing intelligent automation frameworks, security orchestration platforms, and incident response automation methodologies. In addition to automating the cyber security process and developing security monitoring platforms, there should be a threat intelligence mechanism and information sharing mechanism to enhance the collaboration and information sharing between organizations, industries, and governments is a very critical thing to combat and

Table 1
List of related works.

Authors	Paper	Approaches	Finding	Limitation
[6]	Blockchain-assisted cyber security in medical things using artificial intelligence	Combination of blockchain and artificial intelligence (AI).	Blockchain was found to be effective in improving the security of medical records and detecting attacks on medical Internet of Things (IoT) devices.	Data on the security of medical devices is lacking. This makes assessing the efficacy of blockchain-based solutions for enhancing cyber security in medical devices challenging
[24]	A Novel System-Theoretic Matrix-Based Approach to Analyzing Safety and Security of Cyber-Physical Systems	System-theoretic matrix (STM	The STM was useful for spotting possible risks and weaknesses as well as for developing mitigation plans.	The approach has only been used in one case study. For the process to be validated, further case studies are required. The methodology does not address the issue of uncertainty since the cyber-physical system is more complicated, making analysis unpredictable and exposing it to risk.
[25]	An ensemble deep learning model for cyber threat hunting in the industrial Internet of things	LSTM and AE neural networks.	The model was able to detect cyber threats with high accuracy.	The model has only been evaluated on a dataset of Internet of Things (IoT) data from a single industrial control system. The model does not address the issue of false positives.
[26]	Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems	Healthcare 4.0 and blockchain integration with secure cloud-based electronic health record systems	Develop mode secure and safe Model to Reduce the need for manual data entry and offer a safe and efficient means for authorized individuals to access electronic health records (EHRs) using Blockchain technology.	Challenges include the cost of using blockchain technology, the lack of experienced employees to implement and operate blockchain systems, and the lack of standards for data exchange and privacy-preserving mechanisms for data sharing.
[27]	Maximizing the benefits of sharing cyber threat intelligence by government agencies and departments	Develop a theoretical model that demonstrates how the advantages of sharing cyber threat intelligence are directly related to the difference between the danger level indicated by the cyber threat intelligence and the sharing organization's prior assumption about the threat level.	The authors' findings suggest that it is not optimal for government agencies to focus on sharing CTI related to vulnerabilities with the highest threat level. Instead, government agencies should focus on sharing CTI that is likely to have the greatest impact on organizations with lower prior beliefs of the threat level.	The authors' findings are based on a theoretical model and do not provide empirical evidence to support their findings.
[28]	The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation	A qualitative examination of the United States' cyber security strategies to track the evolution of military cyber power theories in the United States.	Identify significant themes and gaps in the United States cyber strategy.	It depends on only US military cyber security departments.
[3]	Cyber threat Detection Using Deep learning approaches for the Internet of Things (IoT)	The researcher uses combined deep learning approaches to detect the cyber security threat of malware attacks.	Cyber threat classification model to classify malware attacks which helps to identify the pirated software used as a weapon for attacking the Internet of Things (IoT) network	Computationally expensive and needs a large dataset, and the researcher does not consider the Adversarial attacks that are purposively done to mislead deep learning models.
[39]	Conducted a comprehensive overview of the use of machine learning (ML) in cybersecurity	Systematic review on the role of machine learning in cyber security.	The paper also discusses the challenges of using ML in cybersecurity, such as the need for large amounts of labeled data, the difficulty of interpreting ML models, and the vulnerability of ML models to adversarial attacks.	The researcher does not address anti-machine learning attacks and their challenges

properly respond to cyber-attacks on the targeted cyber security industries. The researcher, academician, and cyber security experts should be focused on developing standard frameworks and platforms to share cyber threats and bring up collaborative cyber defense mechanisms for organizations, industries, and governments.

Data protection and privacy is a great concern in the digital world and the concern of protecting the data and privacy is increasingly growing. Therefore, privacy regulations, data protection techniques, and privacy-preserving techniques should be strengthened and improved. Hence, the researcher should have to focus on how to strengthen the privacy regulations, and privacy [reserving techniques using multi-party computation and homomorphic encryption technology. In addition to this, the development of blockchain technology is also one of the important concerns to strengthen the cyber security of an organization. Blockchain technology and distributed ladder system provide a great solution for security and decentralized systems and different researcher has researched implementing blockchain technology in different cybersecurity areas such as Transaction [7], supply chain [15], and in medical [6,26]. Even if blockchain technology has a great role in providing security mechanisms for the cyber security domain, there are difficulties and challenges such as immutable or changeless transactions, the vulnerability of smart contact, weakness of protocols used in blockchain technology like consensus protocols such as PoS and PoW for attacks, dependency of external system like oracle is also one of security challenges of Blockchain technology. In order to address or minimize such kind of security problems and challenges in Blockchain technology, there should be taken and implement appropriate security measurements such as applying safe smart contract development methods, implementing powerful consensual protocols, incorporating and integrate privacy-enhancing strategies as needed are all part of this. To create a safe and robust system, it is critical to find a balance between the benefits of blockchain and DLT and the related cybersecurity issues (Fig. 1 and Table 1).

8. Conclusion

Cyber security is the process of protecting and safeguarding computer systems, networks, and data from cyber threats that attach to the confidentiality, integrity, and accessibility of information systems. Cy-

ber security is essential for protecting the safety of individuals and organizations since highly depend on digital technologies. Cyber security is applicable in different application areas such as health centers financial institutions, smart cities, grid systems, government organizations, education, and the military. Cyber securities face different challenges from different sources such as Hackers, cybercriminals, state actors, terrorists, and insiders. The challenges faced by the cyber security industry are defensive AI and Machine learning technology, sophisticated cyber-attacks, reinforcement learning-based cyber-attacks, AI-enabled malware, and the vulnerability of IoT technology, cloud security issues, and the involvement of cryptography. However, future directions, in cybersecurity, such as quantum computing (quantum- secure encryption), biometric authentication, advanced artificial intelligence (AI), and machine learning (ML), may be able to address these issues. To ensure that our digital devices, networks, and data are secure against cyber-attacks, individuals, businesses, and governments must continue to invest in cybersecurity.

Funding

No funding received for this paper.

Author contribution

Wasyihun Sema Admass, and Yirga Yayeh created the initial draft of the paper, Conceptualization, supervision, and methodology based on extensive discussions on each point of Cyber security. Both authors read and approved the fnal manuscript, Abebe Diro Provide Sugustions, re-write the drafts and palagarism detections.

Declaration of Competing Interest

We declare that there are no competing interests that could compromise the objectivity or impartiality of the research. We have no personal, professional, or academic relationships that could be considered as potential conflicts of interest.

Data availability

There is no available data.

References

[1] H. Kavak, J.J. Padilla, D. Vernon-Bido, S.Y. Diallo, R. Gore, S. Shetty, Simulation for cybersecurity: state of the art and future directions, J. Cybersecur. 7 (1) (2021) 1–13, doi:10.1093/cybsec/tyab005.
[2] M.Z. Gunduz, R. Das, Cyber-security on smart grid: threats and potential solutions, Comput. Netw. 169 (2020) 107094, doi:10.1016/j.comnet.2019.107094.
[3] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M.A. Latif, F. Al-Turjman, L. Mostarda, Cyber security threats detection in internet of things using deep learning approach, IEEE Access 7 (2019) 124379–124389, doi:10.1109/ACCESS.2019.2937347.
[4] J. Kaur, K.R. Ramkumar, The recent trends in cyber security: a review, J. King Saud Univ.- Comput. Inform. Sci. 34 (8) (2022) 5766–5781, doi:10.1016/j.jksuci.2021.01.018.
[5] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, S. Mahmood, Cyber security threats and vulnerabilities: a systematic mapping study, Arab. J. Sci. Eng. 45 (4) (2020) 3171–3189, doi:10.1007/s13369-019-04319-2.
[6] M. Alshehri, Blockchain-assisted cyber security in medical things using artificial intelligence, Electron. Res. Arch. 31 (2) (2023) 708–728, doi:10.3934/era.2023035.
[7] G.W. Peters, E. Panayi, Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money, SSRN Electron. J. (2015) 1–33, doi:10.2139/ssrn.2692487.
[8] A.M. Tonge, Cyber security: challenges for society- literature review, IOSR J. Comput. Eng. 12 (2) (2013) 67–75, doi:10.9790/0661-1226775.
[9] R. Sharma, Study of latest emerging trends on cyber security and its challenges to society, Int. J. Sci. Eng. Res. 3 (6) (2012) 1–4.
[10] A. Arabo, Cyber security challenges within the connected home ecosystem futures, Procedia Comput. Sci. 61 (0) (2015) 227–232, doi:10.1016/j.procs.2015.09.201.
[11] J. Jang-Jaccard, S. Nepal, A survey of emerging threats in cybersecurity, J. Comput. Syst. Sci. 80 (5) (2014) 973–993, doi:10.1016/j.jcss.2014.02.005.
[12] L.B. Naik, B. AsSadhan, J.M.F. Moura, T. Saadawi, A. El-Desouki, A.S. Elmaghraby, M.M. Losavio, U. Sanath Rao, R. Swathi, V. Sanjana, L. Arpitha, K. Chandrasekhar, Chinmayi, P.K. Naik, M. Alshehri, N. Ben-asher, C. Gonzalez, M. Alshehrima.alshehri@mu.edu.sa, C. Hemminghaus, . . . S. Ddos, Special Issue on Cyber Security and AI, J. Adv. Res. 41 (5) (2019) 557–559, doi:10.4218/etr2.12236.
[13] R. Maeda, M. Mimura, Automating post-exploitation with deep reinforcement learning, Comput. Secur. 100 (2021) 102108, doi:10.1016/j.cose.2020.102108.
[14] G.D. Rodosek, M. Golling, Cyber security: challenges and application areas, Lect. Note. Logist. (2013) 179–197, doi:10.1007/978-3-642-32021-7_11.
[15] P. Dutta, T.M. Choi, S. Somani, R. Butala, Blockchain technology in supply chain operations: applications, challenges and research opportunities, Transport. Res. Part E: Logist. Transport. Rev. 142 (May) (2020) 102067, doi:10.1016/j.tre.2020.102067.
[16] K. Kimani, V. Oduol, K. Langat, Cyber security challenges for IoT-based smart grid networks, Int. J. Crit. Infrastruct. Prot. 25 (2019) 36–49, doi:10.1016/j.ijcip.2019.01.001.
[17] G. Sabaliauskaite, J. Cui, L.S. Liew, Integrating Autonomous Vehicle Safety and Security Analysis Using STPA Method and the Six-Step Model Autonomous Vehicle Security View Project Autonomous Vehicle Security View Project Integrating Autonomous Vehicle Safety and Security Analysis Using STPA M, 11, 2018 https://www.researchgate.net/publication/326504334.
[18] K. Thakur, M. Qiu, K. Gai, M.L. Ali, An investigation on cyber security threats and security models, in: Proceedings - 2nd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2015 - IEEE International Symposium of Smart Cloud, IEEE SSC 2015, 2016, pp. 307–311, doi:10.1109/CSCloud.2015.71.
[19] G. Srivastava, R.H. Jhaveri, S. Bhattacharya, S. Pandya, P.K.R. Rajeswari, Maddikunta, G. Yenduri, J.G. Hall, M. Alazab, T.R Gadekallu, in: XAI For Cybersecurity: State of the Art, Challenges, Open Issues and Future Directions, 1, 2022, pp. 1–33. http://arxiv.org/abs/2206.03585.
[20] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, K.K.R. Choo, Artificial intelligence in cyber security: research advances, challenges, and opportunities, Artif. Intell. Rev. 55 (2) (2022) 1029–1053, doi:10.1007/s10462-021-09976-0.
[21] Y.-L. Cheng, C.-Y. Lee, Y.-L. Huang, C.A. Buckner, R.M. Lafrenie, J.A. Dénommée, J.M. Caswell, D.A. Want, G.G. Gan, Y.C. Leong, P.C. Bee, E. Chin, A.K.H. Teh, S. Picco, L. Villegas, F. Tonelli, M. Merlo, J. Rigau, D. Diaz, . . . R.H.J. Mathijssen, Smart health and cybersecurity in the era of artificial intelligence, in: Intech, 11, 2016, p. 13. https://www.intechopen.com/books/advanced-biometric-technologies/liveness-detection-in-biometrics.
[22] N.N. Abbas, T. Ahmed, S.H.U. Shah, M. Omar, H.W. Park, Investigating the applications of artificial intelligence in cyber security, Scientometrics 121 (2) (2019) 1189–1211, doi:10.1007/s11192-019-03222-9.
[23] H. HaddadPajouh, A. Dehghantanha, R. Khayami, K.K.R. Choo, A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting, Futu. Gener. Comput. Syst. 85 (2018) 88–96, doi:10.1016/j.future.2018.03.007.
[24] L.S. Liew, G. Sabaliauskaite, N.K. Kandasamy, C.Y.W. Wong, A novel system-theoretic matrix-based approach to analysing safety and security of cyber-physical systems, Telecom 2 (4) (2021) 536–553, doi:10.3390/telecom2040030.
[25] A. Yazdinejad, M. Kazemi, R.M. Parizi, A. Dehghantanha, H. Karimipour, An ensemble deep learning model for cyber threat hunting in industrial internet of things, Digit. Commun. Netw. 9 (1) (2022) 101–110, doi:10.1016/j.dcan.2022.09.008.
[26] H.B. Mahajan, A.S. Rashid, A.A. Junnarkar, N. Uke, S.D. Deshpande, P.R. Futane, A. Alkhayyat, B. Alhayani, Integration of healthcare 4.0 and blockchain into secure cloud-based electronic health records systems, Appl. Nanosci. (Switzerl.) 13 (3) (2023) 2329–2342, doi:10.1007/s13204-021-02164-0.
[27] J. Dykstra, L.A. Gordon, P. Martin, Maximizing the benefits from sharing cyber threat intelligence by government agencies and departments, J. Cybersecur. 1 (2023) 1–12, doi:10.1093/cybsec/tyad003.
[28] E.D. Lonergan, The power of beliefs in US cyber strategy : the evolving role of deterrence, norms, and escalation and Jacquelyn Schneider, J. OfCybersecur. (2023) 1–10, doi:10.1093/cybsec/tyad006.
[29] E.S. Barry, J. Merkebu, L. Varpio, State-of-the-art literature review methodology: a six-step approach for knowledge synthesis, Perspect. Med. Educ. 11 (5) (2022) 281–288, doi:10.1007/s40037-022-00725-9.
[30] C. Tankard, Advanced persistent threats and how to monitor and deter them, Netw. Secur. 2011 (8) (2011) 16–19, doi:10.1016/S1353-4858(11)70086-1.
[31] Prenosil, Advanced persistent threat attack detection : an overview, Int. J. Advancem. Comput. Netw. Secur. – IJCNS 4 (4) (2014) 50–54 https://www.researchgate.net/publication/305956804.
[32] H.J. Hejase, H. Kazan, I. Moukadem, Advanced persistent threats (APT): an awareness review, J. Econ. Econ. Educ. Res. 21 (6) (2020) 1–8, doi:10.13140/RG.2.2.31300.65927.
[33] R. Kaur, M. Singh, A survey on zero-day polymorphic worm detection techniques, IEEE Commun. Surv. Tutor. 16 (3) (2014) 1520–1549, doi:10.1109/SURV.2014.022714.00160.
[34] J. Clark, P.C. Van Oorschot, SoK: SSL and HTTPS: revisiting past challenges and evaluating certificate trust model enhancements, in: *Proceedings - IEEE Symposium on Security and Privacy, V*, 2013, pp. 511–525, doi:10.1109/SP.2013.41.
[35] B. AsSadhan, J.M.F. Moura, An efficient method to detect periodic behavior in botnet traffic by analyzing control plane traffic, J. Adv. Res. 5 (4) (2014) 435–448, doi:10.1016/j.jare.2013.11.005.
[36] B. Guembe, A. Azeta, S. Misra, V.C. Osamor, L. Fernandez-Sanz, V. Pospelova, The emerging threat of ai-driven cyber attacks: a review, Applied Artificial Intelligence, 36, Taylor & Francis, 2022, doi:10.1080/08839514.2022.2037254.
[37] B. Bera, A.K. Das, M.S. Obaidat, P. Vijayakumar, K.F. Hsiao, Y. Park, AI-enabled blockchain-based access control for malicious attacks detection and mitigation in IoE, IEEE Consum. Electron. Maga. 10 (5) (2021) 82–92, doi:10.1109/MCE.2020.3040541.
[38] V. Vouvoutsis, F. Casino, C. Patsakis, On the effectiveness of binary emulation in malware classification, J. Inform. Secur. Applic. 68 (2022) 103258, doi:10.1016/j.jisa.2022.103258.
[39] S.G. Langer, Cyber-security issues in healthcare information technology, J. Digit. Imaging 30 (1) (2017) 117–125, doi:10.1007/s10278-016-9913-x.

Wasyihun Sema Admass(MSc):- Received a B.Sc. Degree in Information Technology from Assosa University in 2017, and the M.Sc.His-research and teaching interests include the theory and application of Machine Learning, the internet of Things, Deep Learning, Computer Vision, Wireless and Network security, and Natural Language processing. I am currently serving as a lecturer at Assosa University

Yirga Yayeh Munay(PhD):- received a B.Sc. degree in Information Technology and an M.Sc. degree in Information Science from Bahir Dar University in Addis Ababa University, Ethiopia in 2009 and 2014, respectively. In 2021, he got his PhD Degree in Electrical Engineering and Computer Science (EECS) from the National University of Technology (NTUT), Taiwan. From 2014 to 2017, he functioned as a full-time lecturer and researcher on issues related to Information Technology in Assosa University, Ethiopia. In addition, he acted as the head of the department of Information technology from 2014 to 2016. From 2016 to 2017, he acted as the coordinator of the Continuous and Distance Education Program (CDEP) for the School of Informatics in Assosa University, Assosa, Ethiopia. Currently, He is an assistant professor at Injibara University, Ethiopia, as a researcher and Research and Community Service Vice Dean for Engineering and Technology College. His-research interests are in the areas of application of deep learning in wireless communication, ad-hoc networks, Resource management, UAV-base station deployment, IoT, Emerging Technologies.

Abebe Diro(PhD,Asst.prof):- He is a Lecturer in cybersecurity at RMIT University. He works closely with the Center for Cybersecurity research and innovation. He is interested in AI-based cyber security at continuum of prevention, detection, and response.