Innovative Reviews in Engineering and Science, ISSN: 3048-8745 Vol. 2, No. 2, 2025 (pp. 20-32)
REVIEW ARTICLE
ECEJOURNALS.IN

Critical Review on Understanding Cyber Security Threats

Ngo Tien Hoa[1], Miroslav Voznak[2]
[1,2]Faculty of Electrical and Electronics Engineering, Ho Chi Minh City University of Technology and Education,Vietnam

KEYWORDS:
Advanced Persistent Threats (APTs);
Cybercriminals;
Malware;
Phishing;
Ransomware;
Threat Detection

ARTICLE HISTORY:
Submitted : 08.10.2024
Revised : 10.11.2024
Accepted : 17.02.2025

https://doi.org/10.31838/INES/02.02.03

Abstract

The evolving landscape of cyber security threats presents a significant 9challenge for individuals, organizations, and nations. This critical review examines the current state of understanding regarding cyber security threats, exploring their nature, sources, and impact. The study categorizes threats into various types, including malware, phishing, ransomware, and advanced persistent threats (APTs), highlighting their mechanisms and the sophistication of recent attacks. It emphasizes the growing complexity of cyber threats due to the increasing interconnectivity of systems and the proliferation of Internet of Things (IoT) devices, which expand the attack surface for malicious actors. The review also discusses the primary sources of cyber threats, which range from independent hackers and organized cybercriminal groups to nation-state actors. It underscores the importance of understanding the motivations behind cyber attacks, such as financial gain, political espionage, and disruption of critical infrastructure. Tthe review analyzes the impact of cyber security threats on various sectors, including finance, healthcare, and critical infrastructure, demonstrating the potential for significant economic and societal harm. The study concludes by highlighting the necessity for robust cyber security strategies, including advanced threat detection, continuous monitoring, and comprehensive incident response plans, to mitigate the risks and enhance the resilience of digital systems against evolving threats.

Author e-mail: mnazri_borhan@ukm.edu.my

How to cite this article: Hoa NT, Voznak M. Critical Review on Understanding Cyber Security Threats, Innovative Reviews in Engineering and Science, Vol. 2, No. 2, 2025 (pp. 20-32).

The Evolving Landscape of Digital Threats

In today's interconnected world, cyber security threats pose an ever-increasing risk to individuals, businesses, and nations alike. As we stride into 2024, the landscape of digital threats is rapidly evolving, necessitating a proactive approach to safeguard our virtual realms. From the proliferation of malware and cybercrime to the looming challenges of quantum computing, the realm of cyber security demands vigilance and strategic countermeasures. This comprehensive guide delves into the top cyber security trends poised to shape the digital frontier in 2024. It explores the integration of machine learning and artificial intelligence in cybersecurity solutions, the rise of mobile device security, and the growing importance of compliance measures. Additionally, from the Fig. 1, it sheds light on emerging threats such as deepfakes and state-sponsored cyberattacks, equipping readers with the knowledge to fortify their digital defenses against these escalating risks [1].

Fig. 1: Best practices of cyber threats

A. Increasing Sophistication

The digital threat landscape has undergone a profound transformation, marked by an escalating sophistication of cyberattacks. Attackers are constantly developing new techniques and strategies to breach security systems, steal sensitive data, or disrupt critical services. This evolution is driven by various factors, including the availability of powerful hacking tools, the proliferation of cybercrime forums, and the rise of nation-state-sponsored hacking groups.

B. Diverse Attack Vectors

Digital threats now encompass a wide range of attack vectors, such as malware, ransomware, and distributed denial-of-service (DDoS) attacks. These attack vectors have become more versatile, with attackers combining multiple methods to achieve their goals. For example, a ransomware attack may begin with a phishing email and escalate to the deployment of malware that encrypts data.

C. Target Variety

Digital threats are no longer limited to traditional targets like large corporations and government agencies. Smaller businesses, healthcare organizations, educational institutions, and even individuals are now prime targets, driven by the desire to create disruption or steal valuable personal information.

D. Nation-State Actors

The involvement of nation-state actors in cyber warfare and espionage has added a new dimension to the digital threat landscape. Countries invest heavily in developing cyber capabilities, and state-sponsored hacking groups have been responsible for some of the most high-profile attacks in recent years. These attacks can have geopolitical implications and blur the line between traditional and cyber warfare.

E. Supply Chain Attacks

Another emerging trend is the rise of supply chain attacks, where attackers target supply chains to compromise the integrity of products and services. Recent incidents, such as the SolarWinds hack, have demonstrated the devastating impact of supply chain attacks, as they can affect organizations and their customers.

F. IoT Vulnerabilities

The expansion of Internet of Things (IoT) devices has ushered in fresh vulnerabilities within the digital threat landscape. Numerous IoT devices exhibit insufficient security capabilities, rendering them susceptible to exploitation by malicious actors.[13] These compromised IoT devices can be harnessed to initiate extensive distributed denial-of-service (DDoS) attacks or breach home networks.

G. AI and Machine Learning in Attacks

Attackers are increasingly leveraging artificial intelligence (AI) and machine learning (ML) to enhance their capabilities. These technologies automate attacks, create more convincing phishing emails, and even identify vulnerabilities in target systems. As AI and ML continue to advance, their role in digital threats is likely to grow.

H. Regulatory and Compliance Challenges

The evolving digital threat landscape has prompted governments and regulatory bodies to introduce new cybersecurity regulations and standards. Organizations now face greater pressure to comply with these requirements, but achieving and maintaining compliance can be challenging, given the dynamic nature of digital threats.

I. Response and Resilience

Building effective incident response and resilience strategies has become paramount. Organizations must focus on preventing attacks and detecting, mitigating, and recovering from breaches. This includes regular security assessments, employee training, and robust incident response plans.

J. Global Collaboration

Given the transnational nature of digital threats, international collaboration has become crucial. Governments, law enforcement agencies, and cybersecurity organizations worldwide are working together to share threat intelligence, track down cybercriminals, and mitigate threats on a global scale.[2-8]

Top Cybersecurity Trends

A. The Emergence of Automotive Cybersecurity Threats

The emergence of automotive cybersecurity threats is a relatively recent but rapidly growing concern in the automotive industry. As vehicles become increasingly connected and autonomous, they are also becoming more susceptible to cyber attacks. Modern vehicles are equipped with numerous electronic control units (ECUs) that communicate with each other and external networks, enabling features such as remote diagnostics, over-the-air updates, and infotainment systems. However, this connectivity creates potential entry points for hackers. The interconnected nature of automotive systems means that vulnerabilities in one component can potentially compromise the entire vehicle. Common vulnerabilities include insecure communication protocols, weak authentication mechanisms, and lack of secure update mechanisms. Cyber threats to automotive systems can take various forms, including remote hacking, physical access, denial of service (DoS),

and data theft. The consequences of automotive cyber attacks can range from inconvenience (e.g., temporary loss of functionality) to severe safety risks (e.g., unauthorized control of critical systems like brakes or steering) and financial implications, such as theft of intellectual property or customer data as given in Fig. 2.

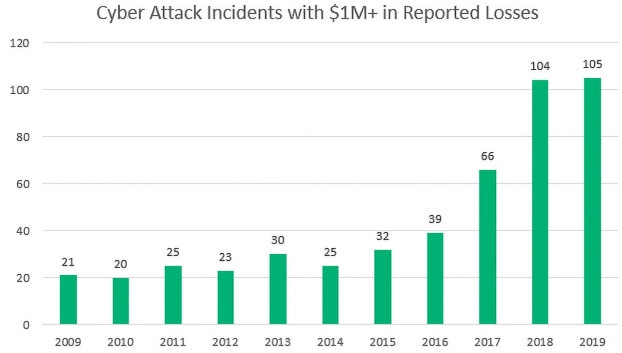

Fig. 2: Cyber attacks year wise

Governments and industry regulators are increasingly recognizing the importance of automotive cybersecurity, with standards and regulations like ISO/SAE 21434 and UNECE WP.29 aiming to establish guidelines for securing connected vehicles and managing cybersecurity risks throughout their lifecycle. Automotive manufacturers, suppliers, and cybersecurity firms are collaborating to develop solutions for mitigating cyber threats, including implementing secure software development practices, conducting regular security assessments, and deploying intrusion detection systems. Despite efforts to enhance automotive cybersecurity, challenges remain, such as the complexity of vehicle software ecosystems, the need for secure supply chains, ensuring timely security updates for legacy vehicles, and balancing security with usability and cost-effectiveness.

B. Harnessing the Power of Artificial Intelligence in Cybersecurity

Artificial Intelligence (AI) has become impossible to ignore when considering any long-term cybersecurity strategy. The technology will inevitably be utilized on both sides of the cybersecurity fight, with malicious actors expected to use AI to increase the rate and sophistication of social engineering attacks, while security teams are heavily investing in AI technology of their own to strengthen their cyber defense.

Cybersecurity is projected to be the fastest-growing category of AI spending at a CAGR of 22.3%. As AI continues to transform the industry, it is expected to be a key catalyst in reducing user risk and boosting security awareness within organizations. Tools like Elevate Engage already help organizations identify and engage their riskiest people to motivate and measure behavior change in near real-time with personalized and automated nudges, controls, and responses. With AI coming to new markets every day, its power is expected to enhance user risk platforms and nudging capabilities to occur faster than ever.

C. Mobile Devices: A Growing Target for Cyber Attacks

Mobile devices have become a prime target for cyberattacks due to their widespread use, increased capabilities, and the valuable data they hold. The sheer number of smartphones and tablets in use worldwide makes them an attractive target for cybercriminals, as more people use these devices for work, communication, banking, and shopping, turning them into repositories of sensitive information. Mobile devices store a wealth of personal and corporate data, including contact lists, emails, messages, photos, and financial information, which is highly valuable to cybercriminals for various malicious purposes, such as identity theft, financial fraud, and corporate espionage. With the rise of mobile banking apps and digital payment systems, mobile devices have become a primary platform for financial transactions, making them targets for stealing banking credentials, credit card information, and conducting unauthorized transactions.

Many organizations allow employees to use their personal devices for work purposes, leading to a mix of personal and corporate data on these devices, increasing the risk of data breaches and exposing sensitive company information to potential cyber threats. Like any software, mobile operating systems (such as iOS and Android) and apps are susceptible to vulnerabilities and security flaws, which cybercriminals exploit through techniques like malware, phishing, and social engineering attacks. Compared to traditional computing devices like PCs, users may be less vigilant about security practices on mobile devices, making them more susceptible to falling for scams, downloading malicious apps, or connecting to unsecured networks. Mobile devices often serve as hubs for Internet of Things (IoT) devices, such as smart home appliances and wearables, and compromising a mobile device can provide attackers with a gateway to infiltrate and control other connected devices within a network.

D. Cloud Security Challenges and Solutions

As technology rapidly develops, the cloud has become synonymous with convenience, scalability, and cost-effectiveness in data management and operations for businesses worldwide. However, this evolution comes with its own set of vulnerabilities – cloud security risks,

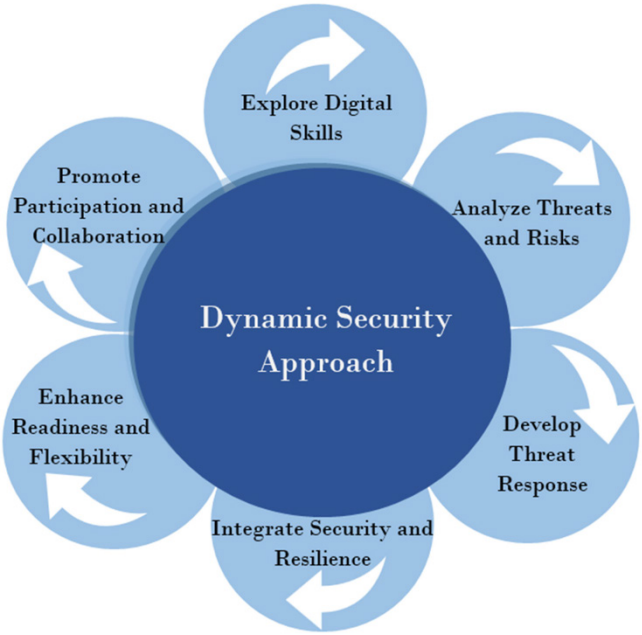

Fig. 3: Counterattacking Cyber Threats

which are potential weaknesses in the cloud infrastructure that could be exploited by cyber attackers, leading to unauthorized access, data breaches, service disruptions, and compliance violations. One of the most pervasive cloud security risks is misconfiguration, where virtual doors are left open due to improper settings, providing easy entry points for attackers. Organizations often underestimate the importance of continuous vigilance and expertise required to maintain cloud configurations properly, leading to accidental exposure of sensitive data or resources as mentioned in Fig. 3.

APIs and interfaces, which are the linchpins of cloud services, are prime targets for attackers due to their accessibility, and insecure APIs can lead to unauthorized access, data leakage, and service manipulation. Ensuring API security necessitates rigorous access controls, encryption in transit and at rest, and regular audits to identify and rectify vulnerabilities. Cloud services often centralize access to resources under specific user accounts or identity credentials, and if an attacker successfully hijacks these credentials, they can access sensitive data, disrupt services, and leverage the cloud resources for malicious purposes, such as launching further attacks. Account hijacking can lead to identity theft, financial fraud, and reputational damage for the affected organization.[9-12]

The human element remains one of the most unpredictable variables in cloud security, with insider threats ranging from negligent employees unintentionally exposing data to malicious insiders intentionally sabotaging systems or stealing information. Given the access privileges necessary for certain roles, insiders can cause significant damage or data loss. Data breaches and data loss represent critical cloud security risks that can have severe consequences for organizations, leading to significant financial losses, reputational damage, and regulatory penalties. Data breaches occur when unauthorized parties gain access to sensitive information stored in the cloud, resulting in theft, manipulation, or exposure, while data loss refers to the unintentional destruction or unavailability of data.

Zero-day exploits, which are vulnerabilities in software or hardware that are unknown to the vendor and have no patch or fix available, pose a significant threat to cloud security as attackers can exploit them to launch targeted attacks without detection. Cyberattacks, such as malware infections, phishing campaigns, ransomware attacks, distributed denial-of-service (DDoS) attacks, and man-in-the-middle (MitM) attacks, target cloud environments due to their rich troves of data and interconnected infrastructure, making them lucrative targets for exploitation. Effective Identity and Access Management (IAM) is the cornerstone of robust cloud security, but inadequate IAM policies can lead to unauthorized access and potential insider threats. As organizations expand and embrace hybrid work environments, managing who has access to what becomes exponentially complex, and excessive permissions significantly increase the risk of data exposure or loss should those credentials be compromised.

Advanced Persistent Threats (APTs) represent a sophisticated, high-level threat wherein an attacker gains unauthorized access to a network and remains undetected for an extended period, targeting the cloud environment for its vast resources and data. APTs can cause significant financial and reputational damage to organizations, emphasizing the need for advanced threat detection and response strategies in the cloud ecosystem. Data security non-compliance, which refers to the failure of organizations to adhere to regulatory requirements, industry standards, or internal policies governing the protection of sensitive data in the cloud, can result in legal penalties, financial sanctions, and reputational damage. Data breaches resulting from non-compliance can erode customer trust and confidence in the organization's ability to safeguard their personal information as shown in Fig. 4.

Other challenges in cloud security include the lack of knowledge and skills required to implement and maintain robust security measures, shadow IT (the use of unauthorized applications and services by employees without the knowledge or approval of the IT

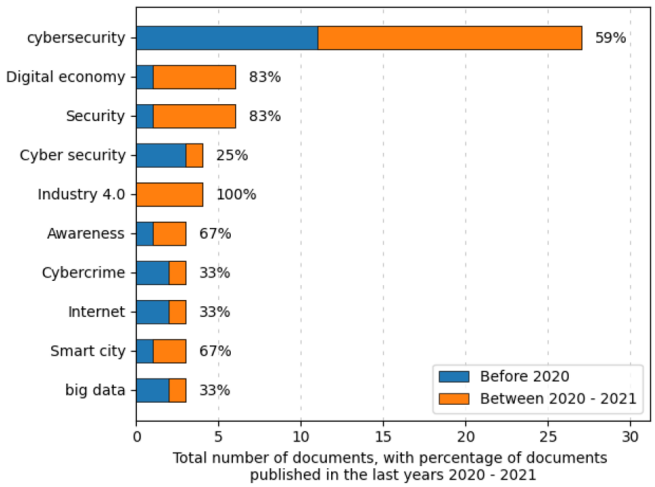

Fig. 4: Global Digital Convergence

department), access management challenges, and the dynamic nature of cloud environments, which creates new opportunities for cyber attackers. The adoption of multi-cloud environments, where organizations utilize services from multiple cloud providers, introduces unique security challenges, such as managing security across diverse cloud platforms, interoperability issues, data migration challenges, and differences in governance models between cloud providers.

E. Data Breaches: A Persistent Concern

Data breaches continue to be a persistent concern in the cybersecurity landscape, with organizations facing significant risks of unauthorized access, data theft, and financial losses. Globally, the exploitation of vulnerabilities as an initial point of entry increased since last year, accounting for 14% of all breaches. The exploitation of zero-day vulnerabilities by ransomware actors remains a persistent threat to enterprises, due in no small part to the interconnectedness of supply chains. Analysis of the Cybersecurity Infrastructure and Security Agency (CISA) Known Exploited Vulnerabilities (KEV) catalogue revealed that on average, it takes organizations 55 days to remediate 50% of critical vulnerabilities following the availability of patches. While the adoption of artificial intelligence to gain access to valuable corporate assets is a concern on the horizon, a failure to patch basic vulnerabilities has threat actors not needing to rapidly advance their approach and focusing their use of AI on accelerating social engineering.

F. IoT Security in the Era of 5G

The coexistence of IoT security and 5G technology is apparent, as 5G networks have unmatched speed, low latency, and huge connections, making them perfect for supporting the large number of IoT devices that are likely to be online in the near future. From smart homes and self-driving cars to industrial automation and healthcare systems, 5G-enabled IoT devices have the potential to transform a variety of industries. However, this interdependence creates serious security challenges, as IoT devices frequently lack effective security features, leaving them open to hackers. With 5G's increasing bandwidth and capacity, the potential impact of security breaches grows, posing privacy threats and data integrity risks.

Integrating IoT devices with 5G networks significantly expands the field for potential cyber threats, as the number of connected devices skyrockets, increasing the potential for vulnerabilities. Each IoT device, ranging from smart home thermostats to industrial sensors, could be a gateway for cyberattacks, and the healthcare sector is particularly at risk with its widespread adoption of IoT for patient monitoring and device management. As IoT devices constantly gather, send, and process enormous amounts of data, concerns about data privacy become increasingly crucial, as the interconnectedness of these devices heightens the risk, and the compromise of even a single device in the network can result in the unintended disclosure of private information.

While 5G networks significantly improve speed and connectivity, they also introduce new security risks from the network's structure and the vast array of devices they support, with the primary concern being the expanded attack surface resulting from increased connectivity and the complexity of managing and securing these devices' identities within the 5G network. However, the advancements in IoT security, bolstered by the introduction of 5G technology, are a leap forward in addressing the intricate security requirements of various IoT systems. 5G technology brings superior security features for IoT networks, such as advanced encryption methods, improved identity management, and sophisticated privacy-preserving tactics, which are critical for protecting data integrity and confidentiality across the network.

With the rollout of 5G, there has been a significant development in IoT security protocols and standards, specifically designed to leverage 5G's strengths, including enhanced authentication and authorization processes, ensuring that only authorized devices and users can access the network. The integration of Mobile Edge Computing (MEC) within these systems is pivotal, allowing for local, real-time data processing, thereby sharply reducing reaction times to security threats

and bolstering security and efficiency of the energy network .[13-15]

G. Embracing Automation for Enhanced Cybersecurity

Automated cybersecurity tools play a pivotal role in combating automated cyber-attacks, and utilizing them is essential for staying ahead of malicious actors, as they can perform tasks beyond human capabilities, saving time and effort in defending against malicious intrusions. Implementing an efficient security program, fortified with automation, is crucial for defending against any form of attack, as cybersecurity automation has gained popularity due to its effectiveness in tackling cyber-attacks without human intervention, enabling security teams to focus on more strategic endeavors. Analytics, intelligence, and automation are essential for transitioning to proactive security, enabling organizations to take control of their environment and schedule. Security automation tools swiftly detect, triage, and resolve security incidents, reducing alert fatigue in security teams and mitigating the impact of attacks. Automation, facilitated through a security framework, helps minimize risks by identifying vulnerable endpoints and establishing parameters for their handling.

Cybersecurity automation tools encompass security automation and orchestration (SOAR) products, robotic process automation (RPA), and software for process automation and analysis. Integrated with artificial intelligence, machine learning, and data analytics, these tools rapidly filter vast amounts of data to detect and mitigate potential threats. Leveraging AI provides better decision-making insight, while machine learning detects and identifies threats, preventing users from being targeted by monitoring network behavior for anomalies. Automation enhances efficiency by enabling quick responses to threats, minimizing the impact on the bottom line. It organizes data to identify threats and necessary actions, crucial for effective cybersecurity. Moreover, automation improves security posture by processing data faster and more accurately, leading to better threat detection and prevention. It is also cost-effective, reducing the need for human intervention and allowing security teams to focus on strategic initiatives. By staying ahead of cyber attackers, organizations can protect their networks and data more effectively, safeguarding against potential breaches.

Utilizing artificial intelligence and other digital technologies provides invaluable insights into the evolving threat landscape, identifying patterns imperceptible to humans. Automated security platforms swiftly analyze data, generating an attack DNA to transform unknown threats into known ones, and can autonomously implement a comprehensive set of protections to thwart future attacks instantly. Automation streamlines the creation of new protection measures, simplifying the process of adapting to evolving cyber threats.

H. Targeted Ransomware Attacks

The ransomware landscape is expected to witness a rise in targeted ransomware attacks against specific industries or organizations, as cybercriminals conduct thorough reconnaissance to identify high-value targets, such as healthcare providers, financial institutions, or critical infrastructure entities, in order to maximize their extortion efforts. Double extortion tactics, where threat actors not only encrypt data but also exfiltrate sensitive information to use as leverage, are anticipated to become more prevalent, increasing the pressure on victims to pay the ransom by threatening to release or sell stolen data if demands are not met.

Supply chain attacks, where cybercriminals exploit vulnerabilities in third-party software or services to gain access to their primary targets, are expected to rise, amplifying the impact of their attacks due to the increasing interconnectedness of global supply chains. The emergence of hybrid ransomware attacks, combining elements of traditional ransomware with other cyber threats such as data manipulation or destructive malware, is likely, aiming to inflict maximum damage on victims by not only encrypting data but also disrupting operations or causing irreversible harm. Ransomware-as-a-Service (RaaS) models are expected to evolve further, offering new features and capabilities to cybercriminals, including improved encryption algorithms, evasion techniques to bypass security controls, and enhanced customer support to facilitate ransom payment and decryption.

I. Escalating State-Sponsored Cyber Warfare

The involvement of nation-state actors in cyber warfare and espionage has added a new dimension to the digital threat landscape, with countries investing heavily in developing cyber capabilities, and state-sponsored hacking groups being responsible for some of the most high-profile attacks in recent years. These attacks can have geopolitical implications and blur the line between traditional and cyber warfare.

In the context of escalating regional tensions, cyber threat groups have solidified utilizing brazen claims during periods of unrest as a means of gaining notoriety, regardless of the validity of their claims. This highlights the importance of threat intelligence that spans and

provides insights across cyber and physical realms, the need for a deep and contextual understanding of all cyber groups involved, including the targets they seek to exploit, their motivations, their affiliations, and their tactics, techniques, and procedures (TTPs), as well as the impact of cyber attacks (and claims) across varying degrees of severity and sophistication.

Groups like Handala Hack, which has been active since at least December 18, 2023, demonstrate a loose affiliation with Anonymous through participation in the #OpIsrael campaign and have primarily carried out low-level website defacements against Israeli public and private institutions aligned with critical infrastructure. They are ideologically motivated and reputation-seeking

Addressing Cybersecurity Challenges

A. Mitigating Insider Threats Through Awareness

Employees are the first line of defense in safeguarding a company's sensitive data, yet they are also its weakest link, and can be easily manipulated by bad actors seeking sensitive data and credentials. The first step in combating social engineering is to recognize the problem and its prevalence. Social engineering attacks manipulate people into sharing information they shouldn't or making other mistakes that compromise their personal or organizational security. Experts from the social and behavioral sciences discussed the contributors to human error and insider threat, including ways to assess the risk of human error (e.g., human reliability analysis), contributing factors to human error, and tools for minimizing the likelihood of human error. This interactive, realistic scenario-based experience focused on enhancing awareness and implementing strategies to counteract insider threats enabled by cyber means.[16]

B. Addressing Cybersecurity Challenges in Remote Work Environments

The seismic shift to remote work in 2020 revolutionized the way businesses operate, offering unparalleled flexibility but also unveiling a myriad of cybersecurity challenges. The absence of control over employees' devices poses a significant risk to cybersecurity. Solution: Enforcing strict device security policies is imperative. Mandating the use of company-provided devices or ensuring personal devices meet specific security standards can mitigate this risk. Seamless connectivity to company resources is paramount for remote work efficiency. However, users often encounter connectivity issues or require timely IT support in case of technical glitches or system compromises. Solution: Deploying robust connectivity solutions with built-in security controls is crucial. Additionally, establishing remote support mechanisms ensures prompt resolution of technical issues, minimizing disruptions and vulnerabilities as in Fig. 5.

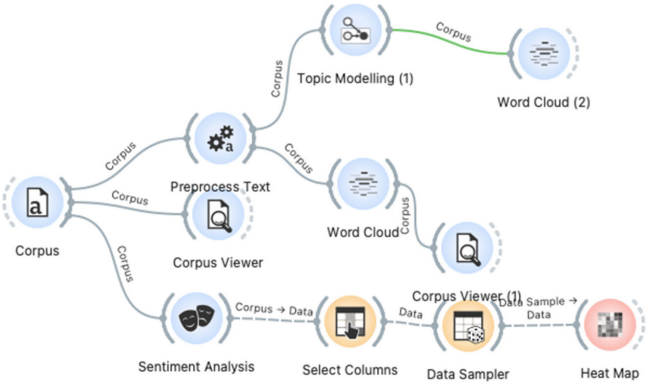

Fig. 5: Heat map flow of cyber attacks

The dispersed nature of remote work environments introduces vulnerabilities in network security, such as unsecured Wi-Fi configurations and physical laptop security lapses. Solution: Enforcing strict Wi-Fi security configurations and implementing endpoint security measures like BitLocker encryption are imperative. Remote employees may not receive adequate cybersecurity training, rendering them susceptible to social engineering attacks and other cyber threats. Solution: Conducting regular cybersecurity awareness training tailored to remote work scenarios is essential. Comprehensive risk assessments specific to remote work processes are indispensable for identifying and mitigating cybersecurity risks effectively. Solution: Evaluating the criticality of information involved and potential risks is fundamental. Implementing necessary controls, such as access restrictions, encryption, and access control mechanisms, based on risk assessment findings enhances the organization's cybersecurity posture.

C. Combating Social Engineering Attacks

Phishing will continue to be the biggest threat to businesses, made even more harmful with Gen AI. Dynamic content (a/k/a adaptive content) in emails through Gen AI is making detecting phishing attempts harder. To avoid phishing emails in the Gen AI era, verify messages from people you know, be careful with MFA prompts you don't recognize, don't click on any attachments or links without verifying the sender, and be wary of urgent language. According to experts, social engineering attacks are predicted to make use of artificial intelligence (AI) technology more frequently in 2024. [46] This will involve the creation of more sophisticated AI tools that can produce deceptive content, as well as advanced

threats such as deepfakes and spear phishing attacks.[46] The integration of AI in social engineering attacks gives cybercriminals enhanced abilities to manipulate and deceive individuals.[46] Password managers are key to combatting social engineering, and the adoption of passkeys will be a crucial step in the eradication of social engineering attacks. When you remove the password, you eliminate the phishable key to your company's data. Ultimately, though, the elimination of passwords will be the strongest defense against a type of attack that manipulates human fallibility.[11-15]

D. Enhancing Security with Multi-Factor Authentication

Multifactor authentication is a security mechanism that requires users to provide two or more forms of authentication to verify their identity before granting access to a system, application, or service. By combining multiple factors, MFA provides an additional layer of security beyond traditional password-based authentication, making it significantly more difficult for unauthorized users to gain access. As cyber threats continue to evolve and become more sophisticated, relying solely on passwords for authentication is no longer sufficient. Passwords are inherently vulnerable to attacks such as phishing, brute force, and credential stuffing. Multifactor authentication mitigates these risks by adding an extra layer of protection, significantly reducing the likelihood of unauthorized access and data breaches.

Implementing biometric authentication methods, such as fingerprint or facial recognition, enhances the security of MFA by leveraging unique physiological characteristics to verify users' identities. Biometric data is difficult to replicate or spoof, providing a high level of assurance in authentication processes. Adaptive authentication utilizes contextual information, such as user behavior, location, and device attributes, to dynamically adjust the level of authentication required based on the perceived risk of the transaction. Utilizing mobile authentication apps, such as Google Authenticator or Microsoft Authenticator, enhances the security and convenience of MFA by generating one-time passcodes that users can use to authenticate their identity. These apps are often more secure than traditional SMS-based authentication methods, as they are less susceptible to interception or phishing attacks. Deploying hardware tokens, such as USB security keys or smart cards, provides an additional layer of security for MFA. Hardware tokens generate unique cryptographic keys that users must possess physically to authenticate their identity, making them resistant to phishing and other remote attacks.

E. Defending Against International State-Sponsored Attacks

The United States and our allies face sophisticated cyber threats from both state and non-state actors. Malicious cyber actors are difficult to observe and attribute. The People's Republic of China (PRC) and the Russia Federation have integrated cyber attack capabilities into military planning and operations to gain advantage during a crisis or conflict. Beijing, Moscow, and Tehran increasingly use social media and state-sponsored disinformation sites, both overt and covert, to shape narratives and sow confusion. The PRC is the only competitor with the intent and, increasingly, the capacity, to reshape the international order. The PRC is the closest competitor in cyberspace and central to the global technology supply chain; it employs the world's largest cyberspace operations workforce and an even larger set of enablers in its defense, cybersecurity, and information technology industries.

Russia's military and intelligence cyber forces are capable and persistent. Their focus on the conflict in Ukraine has diverted, but not ended, their worldwide intelligence and operational efforts in support of Moscow's foreign policy. Russian actors also attempt to divide Western allies and undermine them both abroad and internally. Moscow likely views the upcoming U.S. election as an opportunity for malign influence and has previously targeted elections in the United States and Europe. Iran's growing expertise and willingness to conduct malicious cyber operations make it a threat to the security of U.S. and allied networks. Iranian actors aggressively collect intelligence via the cyber domain, and back Tehran's objectives through cyber attacks, cyber-enabled propaganda, and regime control of domestic Internet access. Iran particularly seeks to increase operations and targeting of industrial control systems to disrupt critical infrastructure.

The DPRK maintains increasingly capable cyber forces comprising both a growing cyber force within its borders and DPRK information technology workers living abroad. Pyongyang's use of cyberspace to collect intelligence, circumvent sanctions, and generate illicit revenue through cryptocurrency exploitation likely supports the regime's nuclear and ballistic missile programs, affecting regional and global security. Non-state actors remain a threat in cyberspace. Cyber criminals, some operating from Russia and with ties to Russian military and intelligence services, continue to find new victims in the United States and globally. USCYBERCOM and the NSA enable efforts by the Department of the Treasury, the Federal Bureau of Investigation (FBI) and other partners

to disrupt ransomware, cryptocurrency theft, and other criminal activities. In addition, violent extremist groups still operate in cyberspace. Though their capabilities have been eroded, the Islamic State in Iraq and Syria (ISIS), al Qaida, and other terrorist groups maintain the intent to target Americans.[16-17]

F. Strengthening Identity and Access Management

Many companies have applications, platforms, and tools that are designed with implicit trust features. Implicit trust means that if users have access to your network or log in to a tool, the system "remembers" them and doesn't always prompt the user to verify their identity again. These lax access permissions can pose a major risk to your organization's security stance if an unauthorized entity gains access to your system via a remembered credential. A Zero Trust security model relies on these core principles: never trust, always verify; assume breach; and apply least-privileged access. By adopting a Zero Trust model and services that work with IAM, companies can always guarantee users are who they claim to be before allowing access to company resources. This constant authentication supports IAM best practices by reducing the risk of unintentionally allowing access to unauthorized users.

Protecting your most valuable data starts by limiting who can access it as much as possible—but, to limit access, you first need to know where your most valuable data is stored and how it is used. Companies identify high-value assets (HVAs) — including data and the systems that house them — based on what data would pose the biggest threat to the organization if it was lost or compromised. Once you've identified your high-value data, it's important to see where it's stored and what applications and tools have access to that data. From there, use access control best practices and policies to limit access to that data and deprovision access from users who don't need that data to do their daily work. Your IAM technologies are only as strong as the identity management best practices and policies that support them. If your team is leveraging single sign-on (SSO) tools, it's critical that each user's password is strong, unique, and difficult to guess to support password and IAM best practices. Passwords must be complex enough to deter cyberattacks, frequently changed, and not used for multiple sign-on requirements.

User authentication is an essential component of effective identity and access management best practices. After all, if you can't guarantee a user is who they claim to be, you may be putting your data at risk and unintentionally allowing access to an unauthorized user. This is crucial for advanced types of attacks like synthetic identity fraud, where the hacker has access to primary identifiable information like a person's name or address. Login credentials alone aren't enough to validate a user's identity; companies need an additional step to ensure the person logging in with those credentials is the authorized user. MFA tools simplify and automate the authentication process by requiring two or more forms of validation to confirm a user's identity. IAM tools offer IT teams many opportunities to use automation to make your organization more secure. Automation reduces manual errors, streamlines workflows, and supports compliance and governance needs. Common tasks like creating accounts, changing passwords, and provisioning or deprovisioning access for personnel changes can easily be automated with IAM technology. These automations support best practices for access control, helping the company stay protected against insider threats when employees leave while also simplifying the transition for new employees or those transitioning into a new role.

One of the most common roles and permissions best practices is applying the principle of least privilege. IAM least privilege encourages organizations to restrict access and permissions as much as possible, without interfering with users' daily workflows. Role management best practices should be used to define the minimum amount of privilege users in each role need to perform their work. It's especially important to limit administrative and change capabilities to ensure single admins don't have excessive permissions they don't need. Divide responsibilities to avoid over-provisioning access to certain people and adopt privileged access management best practices (PAM). Using role-based access control (RBAC) and attribute-based access control (ABAC) together can facilitate robust user access management best practices. RBAC determines access based on a user's role, giving the same access to everyone called a "third-party vendor," "administrator," or "manager" based on their title. ABAC uses policies to define access based on filters and attributes assigned to users. Combining RBAC and ABAC can help automate provisioning and deprovisioning as users join the company, leave the organization, or change roles. Setting up these access control policies is an essential element of IAM implementation best practices.[18-19]

Even with strong policies around access control, over-provisioning remains a problem for many organizations as mentioned in Fig. 6. Auditing is one of the fundamental IAM best practices to build into your overall IAM strategy to maintain the principle of least privilege. Organizations are constantly adding new tools and applications to their tech stack, and employees may believe they need access

Fig. 6: Framework for the Future of Cybersecurity

to all these tools to perform their work. However, as teams streamline their workflows using those tools, IT commonly finds orphaned accounts that employees aren't using. By auditing usage logs and access permissions regularly, IT teams can deprovision access and reduce their attack surface. Many IAM tools automatically generate logs, and these logs are valuable tools to help your team meet compliance requirements, audit usage, and strengthen IAM policies. However, not all teams think to centralize where they store their logs. Rather than pulling logs from multiple locations, many companies store logs on the cloud for easy reference. In an increasingly hybrid work environment, storing logs on the cloud instead of on-premises is often a more convenient and affordable way to keep logs available and accessible. But, when centralizing log collection, companies must consider current cloud IAM best practices to keep valuable log data secure without limiting accessibility.

Using the right tools can make applying identity and access management industry best practices much easier for your organization. There's no need to force a round peg into a square hole; instead of making IAM solutions fit your existing tech stack, search for the right solutions that already support your existing tools and applications. Some tools may need to be reconfigured to support IAM technology. However, IAM implementation best practices recommend that you limit how many reconfiguration projects need to be done to integrate IAM technology. Even as you search for the right tools to support your tech stack, you can start identifying and adopting user account management best practices for your organization long before you have the tools to automate it. Defining those policies early will make it easier to set up your IAM framework and systems later.

G. Real-Time Data Monitoring for Early Threat Detection

Real-time data monitoring for early threat detection is an indispensable tool in the modern landscape of cybersecurity. In today's interconnected world, where businesses rely heavily on digital infrastructure and data flows, the ability to detect and mitigate threats in real-time can mean the difference between safeguarding sensitive information and falling victim to cyberattacks. In such a scenario, real-time data monitoring emerges as a crucial line of defense. By continuously analyzing incoming data streams and network traffic, organizations can identify suspicious patterns or anomalies that may indicate a potential security breach. This proactive approach allows security teams to respond swiftly to emerging threats, minimizing the risk of damage or data loss.[20]

At the heart of real-time data monitoring lies advanced analytics and machine learning algorithms, often integrated into SIEM platforms and XDR solutions. These powerful tools enable organizations to sift through vast amounts of data in real-time, identifying trends, correlations, and outliers that may signal a security threat. By leveraging historical data and predictive modeling, these algorithms can anticipate potential threats before they fully manifest, providing security teams with valuable insights to preemptively shore up defenses. Database Activity Monitoring (DAM) tools play a critical role in monitoring and auditing database transactions and activities in real-time. By analyzing database logs and user activities, DAM tools can detect unauthorized access attempts, data exfiltration, and other suspicious behaviors, helping organizations protect their sensitive data assets.

Endpoint security solutions provide protection for devices such as laptops, desktops, and mobile devices against various cyber threats. These solutions often include features such as antivirus, anti-malware, firewall, and endpoint detection and response (EDR) capabilities, enabling organizations to secure endpoints and prevent unauthorized access to corporate networks. File Integrity Monitoring (FIM) solutions help organizations monitor and detect unauthorized changes to critical system files, directories, and configurations in real-time. By continuously monitoring file integrity and comparing current file attributes with known baseline values, FIM solutions can identify unauthorized modifications, deletions, or additions to files and configurations, providing organizations with early warning signs of potential security incidents or insider threats.

Configuration Integrity Monitoring (CIM) tools help organizations ensure the integrity and security of their IT infrastructure by monitoring and detecting unauthorized changes to system configurations, files, and settings. By continuously monitoring configuration changes in real-time, CIM tools can identify potential security vulnerabilities or unauthorized modifications that may pose risks to the organization's security posture. SOAR platforms enable organizations to automate and orchestrate security operations, allowing them to streamline incident response workflows, automate repetitive tasks, and improve overall operational efficiency. By integrating with existing security tools and technologies, SOAR platforms can enhance the effectiveness of real-time data monitoring by automating incident detection, investigation, and response processes.[21]

Emerging Trends and Future Outlook

A. Ensuring Security for IoT Devices

The rapid adoption of Internet of Things (IoT) devices continues to outpace security measures, leaving major gaps in enterprises' cyber resilience. Each individual connected device presents a potential access point for malicious actors, causing the attack surface to swell to an untenable dimension. IoT attacks grew by a staggering 400% from 2022 to 2023, highlighting the urgency of addressing this issue as given in Fig. 7.

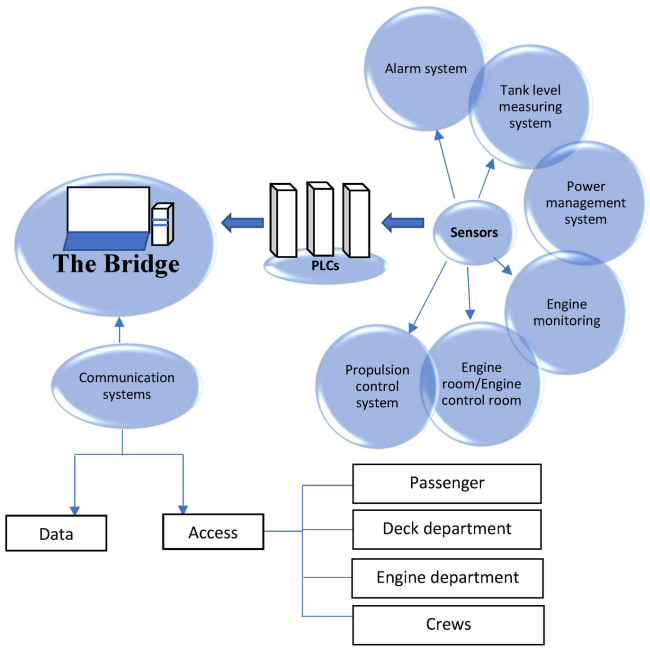

Fig. 7: Cyber Security in the Maritime Industry

IoT vulnerabilities can be somewhat of a blind spot for organizations, with only 43% believing they are "as protected as they can be" from IoT attacks, while 56% agreed that their organizations lack the proper awareness and necessary expertise to prepare for such threats. Organizations that lack confidence in defending their IoT devices should prioritize gaining visibility into the state of IoT security within their enterprise. Product designers and manufacturers should create policies that consider security from the outset of the project, rather than tacking on security measures as an afterthought. IoT devices have finite resources, such as power consumption, processing power, and budgetary constraints, so considering security demands at the beginning can inform product design in terms of hardware, chip selection, and other factors, creating more space for security controls within the device's limitations. Organizations leveraging IoT devices should work to achieve visibility by identifying how many devices are connecting to the network, their connection sources, who operates them, which teams use IoT devices, and which specific devices they are using. Once organizations understand the dynamics of their IoT landscape, they can identify gaps and make a plan to address them, ultimately informing the search for vendors and partners who can provide the most value in securing their IoT ecosystem.

1. **Make certificate outages a thing of the past:** Digital certificates play a crucial role in how IoT devices function, enabling devices to trust the manufacturer's server or API. However, if a certificate expires, the device no longer knows what to trust and essentially ceases to work. The report shows that 98% of organizations experienced a certificate-related outage in the past 12 months, causing losses of more than $2.25 million for the average device manufacturer. These outages are symptoms of a deeper mismanagement of certificate lifecycles, highlighting the need for organizations to prioritize certificate management and renewal.
2. **Define what IoT security looks like and requires for your organization:** Organizations that accomplish visibility by centralizing device identities are better informed in creating their approach to IoT security and implementing policies that maintain that security.
3. **Get ahead of emerging IoT regulations:** Governments and regulating bodies are forming a consensus that IoT security is a shared responsibility, with end users, organizations, and device designers and manufacturers all playing a role in ensuring secure IoT ecosystems. This consensus is slowly but surely distilling into policy,

such as the Biden administration's cybersecurity labeling program for smart products and the Matter standard for smart home devices. 98% of respondents in the IoT report said regulations have an impact on their development of IoT and connected products, indicating the need for organizations to stay ahead of emerging regulations and build crypto-agility within their organizations.

B. Strengthening Cloud Security Measures

Results from global 2024 Cloud Security Outlook studies reveal that 95% of organizations surveyed had cloud-related breaches in the past 18 months, with many organizations harmed by exposed sensitive data. As organizations continue to embrace cloud computing, strengthening cloud security measures has become a critical priority. One approach to enhancing cloud security is the adoption of Cloud-Native Application Protection Platforms (CNAPP). CNAPP solutions can provide proactive protection during runtime, acting as a shared platform for security teams to collaborate with developers and unify, strengthen, and manage DevOps security across multiple pipelines. By centralizing multiple cloud security capabilities under a single umbrella, CNAPP solutions enable security teams to enforce full-lifecycle protections from a centralized dashboard, shifting security left and addressing development risks before they become runtime issue.[22-23]

Microsoft's CNAPP solution, Microsoft Defender for Cloud, has an extended detection and response (XDR) integration that provides richer context to investigations, allowing security teams to gain a comprehensive view of attacks across cloud-native resources, devices, and identities. Approximately 6.5% of Defender for Cloud alerts were connected to other domains, indicating cyberattacks that stretched across multiple cloud products and platforms. Rather than relying on individual point solutions to manage cross-cloud workload threats, organizations need a centralized approach to contextualize findings across their various security approaches. A CNAPP delivers that unified visibility, enabling organizations to address risks more effectively.

One such risk is the presence of unused or unnecessary permissions, known as "super identities." Security teams can drive visibility across the multicloud estate using Cloud Infrastructure Entitlement Management (CIEM) solutions, eliminating the need for standing access for super identities, inactive identities, and unused permissions. In 2023, only 2% of human and workload identity permissions were used, meaning the remaining 98% of unused permissions opened organizations up to unnecessary risk. By using CIEM to identify and revoke unnecessary entitlements, organizations can adopt a just-in-time approach, allowing only the necessary permissions and significantly mitigating potential risks. To address data security risks in the cloud, organizations should deploy integrated solutions through a multilayered approach that combines user and data insights to drive more proactive data security. Microsoft Purview, a comprehensive data security, compliance, and governance solution, can discover hidden risks to data wherever it lives or travels, protect and prevent data loss, and investigate and respond to data security incidents. It can also help improve risk and compliance postures and meet regulatory requirements.

Conclusion

The ever-evolving landscape of cybersecurity threats demands a proactive and multifaceted approach to safeguarding digital assets. As we stride into 2024, organizations must embrace cutting-edge technologies, robust security practices, and a relentless commitment to staying ahead of malicious actors. By harnessing the power of automation, artificial intelligence, and real-time monitoring, we can fortify our defenses against the onslaught of cyber threats, from ransomware attacks to state-sponsored cyber warfare. Collaboration, awareness, and continuous adaptation will be the cornerstones of effective cybersecurity strategies. Fostering international cooperation, cultivating a security-conscious workforce, and staying abreast of emerging trends will be crucial in navigating the complex challenges that lie ahead. By embracing a holistic and forward-thinking mindset, we can build a resilient digital ecosystem, one that protects our invaluable data, preserves our privacy, and safeguards the integrity of our interconnected world.

References: 3

1. Elsayed, S., & Hoque, N. (2021). Cyber threat intelligence: A systematic review. Computers & Security, 103, 102158.
2. Alazab, M., & Tang, M. (2019). Deep learning applications for cyber security. Journal of Information Security and Applications, 41, 1-10.
3. Liao, Y., & Chu, C. H. (2020). Understanding and mitigating ransomware attacks: A survey. Journal of Network and Computer Applications, 104, 102639.
4. Apostolopoulos, T., & Polychronakis, M. (2020). Understanding the prevalence and impact of credential stuffing attacks. Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 1799-1813.
5. Gibson, D., & Igwe, E. (2020). Cybersecurity threats to critical infrastructure. International Journal of Critical Infrastructure Protection, 29, 100367.

6. Bada, M., & Nurse, J. R. C. (2019). The social and psychological impact of cyber-attacks. Frontiers in Psychology, 10, 890.
7. Rani, B. M. S., et al. "Disease prediction based retinal segmentation using bi-directional ConvLSTMU-Net." Journal of Ambient Intelligence and Humanized Computing (2021): 1-10.
8. Bhardwaj, A., & Bhardwaj, A. (2019). Ransomware: A rising threat of new age digital extortion. International Journal of Recent Technology and Engineering, 8 (3), 5945-5948.
9. Babu, D. Vijendra, et al. "Digital code modulation-based MIMO system for underwater localization and navigation using MAP algorithm." Soft Computing (2023): 1-9.
10. Selvam, L., et al. "Collaborative autonomous system based wireless security in signal processing using deep learning techniques." Optik 272 (2023): 170313.
11. Chen, T. M., & Robert, L. P. (2020). Detecting phishing attacks in the digital age. IEEE Transactions on Reliability, 69 (3), 1112-1121.
12. Conti, M., Dragoni, N., & Gottardo, S. (2016). A survey of man in the middle attacks. IEEE Communications Surveys & Tutorials, 18 (3), 2027-2051.
13. Verma, R., & Das, S. (2020). Cyber espionage: Analysis of current threats and defenses. Computers & Security, 94, 101845.
14. Pittala, C.S., et al., "1-Bit FinFET carry cells for low voltage high-speed digital signal processing applications," Silicon, 15(2), 2023, pp.713-724.
15. Faghani, M. R., & Nguyen, T. (2019). Detection and analysis of modern malware: A review of state-of-the-art approaches. Security and Communication Networks, 2019, 1-12.
16. Fernandez, M., & Christodorescu, M. (2021). Advanced persistent threats: Understanding the landscape and challenges. ACM Computing Surveys, 54 (7), 1-34.
17. Gade, S., & Reddy, Y. V. (2020). An overview of phishing attack detection methods. Materials Today: Proceedings, 33, 3280-3283.
18. Li, Y., & Deng, R. H. (2019). A survey on advanced persistent threat: Techniques, solutions, and challenges. IEEE Communications Surveys & Tutorials, 21 (2), 1855-1877.
19. Vijay, V. and Srinivasulu, A., "A novel square wave generator using second-generation differential current conveyor," Arabian Journal for Science and Engineering, 42(12), 2017, pp.4983-4990.
20. Osmanoglu, E., & Kose, B. (2021). The role of artificial intelligence in cyber security threats and defense strategies. Journal of Information Security and Applications, 58, 102690.
21. Shen, C., & Du, X. (2021). A review of Internet of Things (IoT) security: Threats, challenges, and solutions. IEEE Internet of Things Journal, 8 (15), 12215-12232.
22. Rani, B.M.S., et al., "Road Identification Through Efficient Edge Segmentation Based on Morphological Operations," Traitement du Signal, 38(5), 2021.
23. Nizam, Taaha, et al. "Novel all-pass section for high-performance signal processing using CMOS DCCII." TENCON 2021-2021 IEEE Region 10 Conference (TENCON). IEEE, 2021.