International Journal of Scientific Research in Multidisciplinary Studies
Vol.**10**, Issue.**5**, pp.**107-119**, May **2024**
E-ISSN: 2454-9312 P-ISSN: 2454-6143
Available online at: www.isroset.org

Research Article

Cybersecurity Support in IoT: Causes and Solutions in Engineering

Arun Kumar Singh[1*], **Alak Kumar Patra**[2]

[1]School of MCS, PNG University of Technology, Lae, Papua New Guinea
[2]School of Civil Engineering, PNG University of Technology, Lae, Papua New Guinea

**Corresponding author: arunsinghiiita@gmail.com*

Received: 28/Mar/2024; **Accepted**: 30/Apr/2024; **Published**: 31/May/2024

Abstract—The protection of internet-connected devices and the data they generate a crucial aspect of IoT cybersecurity. With the increasing number of devices connected to the internet, the risk of cyber attacks targeting these devices has also grown. Therefore, it is vital to implement security measures to safeguard them. IoT devices are susceptible to various types of attacks, including data theft, unauthorized access, and tampering. These attacks can have severe consequences for individuals and organizations alike. To combat these threats, IoT cybersecurity involves the implementation of measures like encryption, secure authentication, and regular software updates. Protecting IoT devices is not only important for the devices themselves but also for the sensitive data they collect and generate. This data can include personal health information, financial data, or industrial control system data, which makes it an attractive target for cybercriminals. Increasing number of IoT devices and their significant role in our daily lives, it is crucial to prioritize IoT cybersecurity to ensure the privacy, security, and reliability of both the devices and the data they generate. Securing the abstract nature of IoT and the complex systems involved poses a challenge, as they create numerous vulnerabilities that malicious actors can exploit. IoT cybersecurity is crucial to guarantee the confidentiality, integrity, and availability of data and connected devices, as well as protect them from cyber threats like unauthorized access, data theft, and tampering. This article tackles these challenges and suggests various security measures that can be implemented, such as encryption, secure authentication, and regular software updates. Furthermore, specialized IoT security platforms provide comprehensive protection against different cyber threats. These platforms offer features like threat detection and response, access control, and secure communication protocols.

Keywords—Cyber, Security, IoT, Internet

1. Introduction

The significance of cybersecurity in the Internet of Things (IoT) cannot be emphasized enough. With the growing number of interconnected devices, the potential risks associated with these devices also increase. It is crucial for individuals and organizations to be conscious of the possible threats and take necessary actions to safeguard their devices and data. By implementing strong cybersecurity measures, we can ensure that the advantages of IoT are realized while minimizing the risks. The concern for cybersecurity in IoT is a crucial one in the present world, as more and more devices are being connected to the internet. The emergence of smart homes, wearables, and industrial IoT devices has significantly amplified the risk of cyberattacks targeting these devices. Cybersecurity in IoT entails the implementation of security measures to shield internet-connected devices from unauthorized access, theft, and harm. These measures can include encryption, secure authentication, and regular software updates to address security vulnerabilities [1].

However, securing IoT devices can be a daunting task due to their diverse nature, which makes it challenging to establish a standardized security approach. Furthermore, IoT devices often possess limited processing power, memory, and battery life, posing a significant challenge in implementing security measures without compromising performance. Additionally, many IoT devices are designed with user-friendliness in mind, which can result in security vulnerabilities like weak passwords and default credentials. To tackle these challenges, cybersecurity experts are actively working on developing novel security solutions, such as lightweight cryptography, blockchain-based security, and AI-powered threat detection systems. These solutions aim to enhance the security of IoT devices while minimizing the impact on performance and user experience. As the number of IoT devices continues to grow, the importance of cybersecurity in IoT will only increase, and the demand for robust security solutions will become even more critical. Cybersecurity in IoT is a critical area of concern as the internet connects an ever-growing number of devices, including smart home devices, wearables, industrial machinery, and medical devices. The risks associated with these devices being connected to the internet are vast, including data theft, unauthorized access, and tampering. Cybersecurity in IoT strives to protect these devices from such attacks by implementing security measures such as encryption, secure authentication, and regular software updates[2].

One of the unique challenges of cybersecurity in IoT is that many of these devices are designed with limited computing power and memory, making it difficult to implement robust security measures. Additionally, many of these devices are designed to be used for years or even decades, which means that they need to be updated and patched for security vulnerabilities over the long term. To address these challenges, the cybersecurity community is developing new techniques and tools to secure IoT devices, including machine learning-based anomaly detection, distributed denial-of-service (DDoS) protection, and network segmentation [3].

2. Key Considerations of Cyber Security Support

The Internet of Things (IoT) refers back to the network of bodily gadgets, motors, home appliances, and different items embedded with electronics, software program, sensors, and connectivity that allow them to connect and change information with every different and other structures. While IoT offers severa blessings, it also poses tremendous cybersecurity challenges because of the big wide variety of gadgets and their numerous range of skills. The Internet of Things (IoT) presents a unique set of challenges for cybersecurity due to the large range of connected gadgets and the various variety in their competencies. IoT devices can include everything from simple sensors to complex scientific equipment and industrial manage systems. The Internet of Things (IoT) has brought a new set of security challenges because of the large number of linked devices and the diversity in their use instances. As an AI language model, I actually have found that IoT guide in cybersecurity is vital for shielding gadgets, networks, and statistics from cyber threats [4]. IoT (Internet of Things) gadgets have grow to be increasingly popular and are being utilized in houses, businesses, and industries to make our lives less difficult and greater convenient. However, these devices also can pose a substantial cybersecurity danger if they are now not well secured. IoT (Internet of Things) gadgets have become an increasing number of famous in latest years and are being utilized in a wide variety of industries, which include healthcare, production, transportation, and more [5].

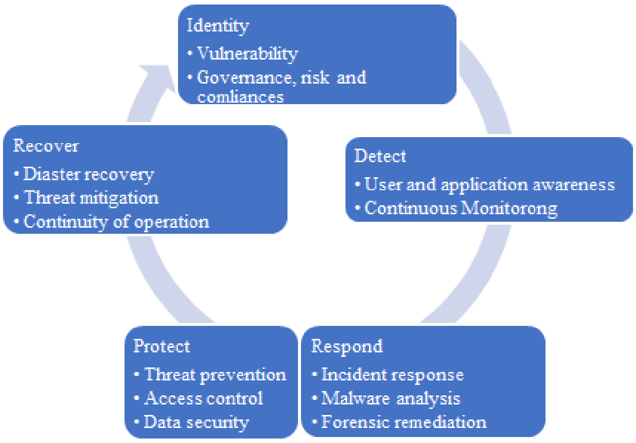

Figure 1. Key Considerations of Cyber Security Support

To support IoT security, there are several key considerations:

- Secure conversation: IoT devices must be capable of communicate securely with each different and with different systems, the use of encryption and different safety mechanisms to guard records in transit.
- Access manipulate: Access to IoT gadgets and networks need to be carefully controlled to prevent unauthorized get right of entry to and ensure that simplest authorized users and gadgets can engage with them.
- Authentication: IoT gadgets have to be capable of authenticate themselves to other devices and structures to make certain that most effective relied on gadgets can access sensitive data and sources.
- Data privateness: IoT gadgets collect and transmit large quantities of facts, plenty of which can be touchy or non-public in nature. This information need to be protected towards unauthorized get entry to, theft, and other threats.
- Patch control: IoT gadgets ought to be frequently updated with safety patches and software updates to address vulnerabilities and other safety problems.
- Monitoring and logging: IoT devices and networks ought to be monitored and logged to come across and respond to safety incidents and other threats in a well timed manner.
- Security by using Design: IoT gadgets have to be designed with security in thoughts from the start, inclusive of functions consisting of robust encryption, steady boot, and get right of entry to manage mechanisms.
- Network Segmentation: IoT gadgets have to be isolated from different gadgets on the network, and traffic among them must be carefully monitored and constrained to save you unauthorized get right of entry to.
- Authentication and Authorization: IoT devices ought to use strong authentication mechanisms to make certain that simplest authorized customers can get admission to them, and authorization rules have to be put in location to restrict the actions that may be taken on the device.
- Patching and Updating: IoT devices ought to be kept updated with the present day safety patches and firmware updates to mitigate vulnerabilities that may be determined after deployment.
- Threat Intelligence: Organizations must monitor and examine chance intelligence feeds to become aware of and respond to new and emerging threats focused on IoT devices.
- Encryption: Data transmitted between IoT gadgets should be encrypted to save you interception and tampering. Additionally, saved information ought to be encrypted to prevent unauthorized get right of entry to in the event of a facts breach.
- Patch Management: Because of outdated firmware and software, Internet of Things devices are often vulnerable to cyberattacks. Updates and patches on a regular basis can assist to fix vulnerabilities and ensure that devices don't crash.
- Network Segmentation: IoT devices should be segmented into separate networks to reduce the chance of a

unmarried compromised device affecting the complete community.

- Monitoring: Continuous monitoring of IoT devices and networks can stumble on anomalies and capability cyber-assaults earlier than they are able to cause considerable harm.
- Physical Security: IoT devices have to be physically secured to prevent unauthorized get entry to and tampering. This consists of measures including tamper-evident seals, protection cameras, and get entry to controls.
- Authentication and Authorization: IoT gadgets have to be configured with strong authentication and authorization mechanisms, including multi-component authentication and position-based totally access control, to make certain that handiest legal customers can get admission to and manage them.
- Secure Device Authentication: IoT guide can provide stable tool authentication, that is the manner of verifying the identity of an IoT tool earlier than allowing it to hook up with a network. This ensures that best legal gadgets are allowed to get entry to the community, preventing unauthorized get right of entry to by cybercriminals.
- Encryption: IoT guide also can provide encryption, that is the system of changing information right into a code to save you unauthorized get entry to. Encryption can help protect records in transit and facts at rest on IoT devices.
- Monitoring and Detection: IoT guide can offer non-stop tracking and detection of capacity threats to IoT devices. This includes identifying anomalies in community site visitors, detecting malicious pastime, and alerting security groups to capacity security breaches.
- Regular Updates: IoT support can make certain that devices acquire ordinary updates and patches to deal with vulnerabilities and mitigate protection risks. This includes updating firmware and software program, in addition to making use of protection patches as they turn out to be available.
- Security Standards and Guidelines: IoT help can provide steerage on safety fine practices and industry standards, inclusive of the NIST Cybersecurity Framework, to assist make sure that IoT gadgets are designed and deployed securely.
- Secure Communication Protocols: IoT gadgets ought to use stable communique protocols, including Transport Layer Security (TLS) or Secure Sockets Layer (SSL), to ensure that statistics transmitted among devices is encrypted and protected from unauthorized get entry to.
- Strong Authentication and Authorization: IoT devices ought to use robust authentication and authorization mechanisms, such as two-element authentication and get admission to controls, to make sure that best authorized users or devices can get right of entry to the tool.
- Regular Security Updates: IoT devices ought to acquire regular safety updates from the manufacturer to make certain that any vulnerabilities are addressed right away.
- Network Segmentation: IoT gadgets must be positioned on separate networks, isolated from crucial structures and records, to save you attackers from transferring laterally throughout the network if an IoT tool is compromised.
- Monitoring and Analytics: IoT gadgets have to be monitored and analyzed to discover any suspicious activity or anomalies which could imply a protection breach.
- Secure Development Practices: IoT gadgets should be evolved the use of secure coding practices and go through rigorous security checking out to make certain that they're not prone to common attacks, which include buffer overflows or injection assaults.

Supporting IoT safety requires a multi-layered technique that mixes technical controls, policies and strategies, and workforce schooling and cognizance [6]. By taking a complete approach to IoT security, organizations can limit their risk of protection breaches and make sure the protection and privateness in their information and structures. IoT assist in cybersecurity requires a multi-faceted approach that entails a mixture of technical, operational, and organizational measures to make certain the security of connected devices and the facts they gather and transmit [7].

3. IoT Support Can Enhance Cybersecurity

Here are some of the ways in which IoT support can enhance cybersecurity:

The Internet of Things (IoT) is a system of interconnected devices and objects that are linked to the internet, enabling them to exchange information and carry out tasks without human intervention. Although IoT devices offer numerous advantages, they also pose specific security challenges. One major concern regarding IoT devices is their often inadequate or non-existent security measures, which make them susceptible to cyberattacks. Hackers can exploit vulnerabilities in these devices to gain unauthorized access to networks, steal sensitive data, or even launch larger-scale attacks. A significant issue with IoT is the lack of basic security features in many devices, such as secure communication protocols and encryption. This renders them vulnerable to hacking, malware, and denial-of-service (DoS) attacks. Moreover, a considerable number of IoT devices are designed to collect and transmit sensitive data, including personal health information, which can be compromised if not adequately protected [8]. To mitigate these security concerns, it is crucial to design and develop IoT devices with security as a priority, and to implement appropriate cybersecurity measures. This involves incorporating robust encryption, secure authentication and access controls, and regular software updates. In addition to these technical measures, organizations should establish security policies and best practices for the usage of IoT devices. This includes restricting access to sensitive data, monitoring devices for suspicious activity, and regularly evaluating and updating security policies. The term "Internet of Things" (IoT) refers to a network of internet-connected devices that can interact with each other. These devices are often embedded in everyday objects, such as household appliances, vehicles, and even medical equipment. Although IoT provides numerous benefits, such as enhanced efficiency and convenience, it also introduces new cybersecurity challenges.

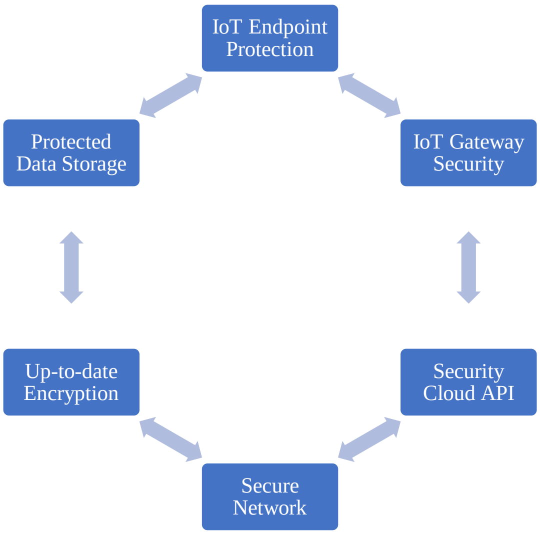

Figure 2. IoT Security Key Recommendations

To tackle these challenges, cybersecurity experts must adopt a comprehensive approach that encompasses both technical and non-technical measures. Some technical measures that can be implemented to secure IoT devices include:

- Authentication and access control: All IoT devices should undergo authentication and obtain authorization before accessing the network. This can be achieved through strong passwords, two-factor authentication, and biometric authentication.
- Encryption: All data transmitted between IoT devices and the network should be encrypted to prevent unauthorized access and tampering.
- Network segmentation: IoT devices should be segregated onto separate networks from other devices to reduce the risk of a single compromised device compromising the entire network.
- Patch management: All IoT devices should be regularly updated with the latest security patches and firmware updates.

In addition to these technical measures, non-technical measures, such as employee training and awareness, can also be effective in preventing IoT attacks. This includes educating employees on how to identify phishing attacks and how to secure their personal devices that are connected to the same network as IoT devices. Overall, securing IoT devices requires a comprehensive approach that combines both technical and non-technical measures. By implementing these measures, organizations can help protect their IoT devices from cyber threats and ensure the privacy and security of their data. IoT support in cybersecurity is critical to ensure the security of connected devices, networks, and data. By implementing the above measures, organizations can significantly reduce the risk of cyber-attacks and protect their assets from potential harm. IoT support can play a vital role in improving cybersecurity by providing secure device authentication, encryption, monitoring and detection, regular updates, and security standards and guidelines. By implementing these measures, organizations can help mitigate the risks associated with IoT devices and better protect their networks and data from cyber threats. Overall, IoT support in cybersecurity requires a combination of technical and procedural measures to ensure that IoT devices are secure and do not pose a risk to the organization.

4. Cybersecurity and Possible Threats

Cybersecurity is an increasingly more crucial problem in present day virtual world, wherein companies and people are facing a developing number of sophisticated and persistent cyber threats. An analytical view of cybersecurity involves information the underlying causes and motivations of those threats, in addition to the techniques and technology that may be used to mitigate them. One of the important thing factors that force cyber threats is the ability monetary gain for attackers. Cyber criminals can income by stealing private or corporate statistics, consisting of monetary data or intellectual property, or through disrupting operations thru ransomware or different kinds of malware. Nation-states can also interact in cyber espionage or sabotage for political or strategic purposes. To deal with those threats, companies need to take a multi-layered method to cybersecurity, with measures that span prevention, detection, reaction, and restoration. This method entails a aggregate of technical answers, together with firewalls, antivirus software, and intrusion detection structures, in addition to regulations and procedures, inclusive of worker education and recognition applications, incident response plans, and hazard management frameworks. Additionally, analytics can play a essential role in cybersecurity, imparting organizations with the potential to monitor and detect threats in actual-time, in addition to to become aware of styles and tendencies that could suggest an coming near near assault. For example, system learning and synthetic intelligence algorithms may be used to analyse big volumes of facts and pick out anomalous behaviourur that could indicate a protection breach. In summary, an analytical view of cybersecurity entails know-how the motivations and strategies of cyber attackers, implementing a multi-layered technique to security, leveraging analytics to come across and reply to threats, and maintaining a way of life of continuous improvement and vigilance. By taking these steps, corporations can protect their belongings and mitigate the dangers of cyber threats [9].

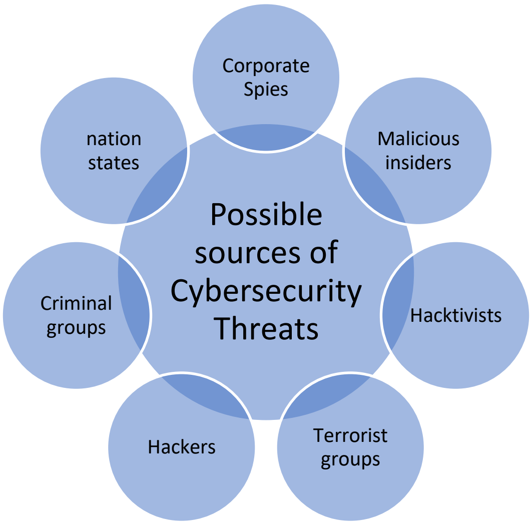

Figure 3. Cybersecurity and Possible Threats

Cybersecurity is the practice of defensive pc systems, networks, and sensitive facts from unauthorized access, use, disclosure, disruption, modification, or destruction. With the increasing dependence on technology and the upward thrust of virtual transformation, cybersecurity threats have become extra frequent and complex. Here are some of the viable threats that cybersecurity experts ought to be aware about:

- Malware: Malware is malicious software program designed to infiltrate or harm a laptop machine. This consists of viruses, worms, and trojan horses. Malware can cause vast damage to structures and data, frequently ensuing in facts breaches or economic loss.
- Phishing: Phishing is a form of social engineering assault where attackers use fraudulent emails, texts, or websites to trick people into presenting touchy facts, along with usernames, passwords, and credit card info.
- Ransomware: Ransomware is a kind of malware that encrypts facts on a sufferer's pc, making it unusable till a ransom is paid. Ransomware assaults have become an increasing number of common and feature resulted in tremendous economic losses for businesses.
- Distributed Denial of Service (DDoS): A DDoS attack is wherein an attacker floods a machine or network with visitors, making it unavailable to users. DDoS assaults are often used as a distraction at the same time as attackers perform other malicious activities, inclusive of stealing touchy information.
- Insider Threats: Insider threats discuss with people inside an enterprise who deliberately or by chance compromise the security of systems or records. This can include personnel who misuse their get right of entry to privileges or accidentally introduce malware to the machine.
- Zero-day vulnerabilities refer to security holes in hardware or software that are not readily apparent to the public or seller. These vulnerabilities can be exploited by attackers to get sensitive data or cause structural damage.
- Advanced Persistent Threats (APTs): APTs are cutting edge, targeted attacks in which the attacker gains access to a device or network and remains hidden for a long time, usually with the intention of stealing confidential data or intellectual property.Malware: Malware is a kind of malicious software program that is designed to damage or gain unauthorized get entry to to computer systems or networks. Examples of malware encompass viruses, trojans, and ransomware.
- Phishing: Phishing is a form of social engineering attack wherein attackers send faux emails or messages to trick users into revealing touchy records, such as passwords or credit score card numbers.
- Insider threats: Insider threats arise when a person with authorized get entry to to a device or network uses that access to steal or misuse touchy facts or reason damage to the gadget or network.
- Distributed Denial of Service (DDoS) attacks: DDoS assaults occur whilst attackers flood a network or server with site visitors to weigh down it and make it unavailable to valid customers.
- Advanced Persistent Threats (APTs): APTs are lengthy-time period, targeted attacks with the aid of skilled hackers who advantage unauthorized get right of entry to to a device or community and continue to be undetected for an extended time frame.
- Zero-day attacks: Zero-day attacks arise while attackers make the most a previously unknown vulnerability in software program or hardware earlier than the vendor has had a hazard to release a patch.
- Crypto jacking: Crypto jacking is a form of assault in which attackers use the computing electricity of a sufferer's device to mine cryptocurrencies with out their knowledge or consent.
- Internet of Things (IoT) assaults: IoT gadgets, along with clever domestic devices or medical devices, are vulnerable to cyber attacks in the event that they lack proper safety features. An assault on an IoT device can result in statistics theft, tool manipulate, or maybe bodily damage to the person.
- Cyber espionage: Cyber espionage involves the theft of sensitive statistics or highbrow property from companies or governments. This can be carried out by means of state-backed hackers or cybercriminals looking for financial gain.

These are only a few examples of the many cybersecurity threats that people and businesses face these days. It is crucial to take a complete technique to cybersecurity, including technical measures which include firewalls, antivirus software, and intrusion detection systems, in addition to non-technical measures inclusive of employee training and cognizance applications. By taking a proactive technique to cybersecurity, organizations can better protect their structures and facts from these and other cyber threats. To prevent these and different cybersecurity threats, companies must enforce a number of security measures, along with frequently updating software program and structures, imposing strong get entry to controls, tracking networks for suspicious pastime, and instructing personnel on cybersecurity high-quality practices [10].

5. CYBERSECURITY THREATS WITH CAUSES

There are numerous cybersecurity threats that can impact organizations, individuals, and governments. Here are some common cybersecurity threats and their causes:

- Phishing attacks: Phishing attacks are a common threat to organizations and individuals. Phishing attacks typically involve an attacker sending an email or message that appears to be from a trusted source, such as a bank or a business, to trick the recipient into providing sensitive information. The cause of phishing attacks is usually social engineering, where attackers exploit human psychology to deceive their targets.
- Malware: Malware is a type of software designed to harm computer systems and networks. Malware can take many forms, including viruses, worms, Trojans, and ransomware. The causes of malware attacks are usually a lack of proper cybersecurity protocols or user error, such as downloading files or software from untrusted sources

or not keeping software up-to-date with the latest security patches.

- Denial of Service (DoS) attacks: DoS attacks are designed to flood a network or server with traffic to the point where it becomes unavailable to users. DoS attacks are usually carried out using botnets, which are networks of infected computers controlled by the attacker. The cause of DoS attacks is usually a lack of proper network security measures or vulnerabilities in network software or hardware.
- Advanced Persistent Threats (APTs): APTs are targeted attacks that are carried out by skilled attackers using sophisticated techniques. APTs are often carried out by state-sponsored hackers or organized cybercriminals seeking to steal sensitive information or intellectual property. The cause of APTs is usually a lack of proper cybersecurity protocols or vulnerabilities in network software or hardware.
- Insider threats: Insider threats are cybersecurity threats that come from within an organization. Insider threats can be malicious, such as theft or sabotage, or unintentional, such as accidental disclosure of sensitive information. The causes of insider threats are usually a lack of proper security protocols, employee training, or inadequate background checks.
- Internet of Things (IoT) attacks: IoT devices are vulnerable to cyber attacks if they lack proper security measures. IoT attacks can result in data theft, device control, or physical harm to the user. The causes of IoT attacks are usually a lack of proper security protocols, vulnerabilities in IoT device software or hardware, or inadequate user training.

These are just a few examples of the many cybersecurity threats and their causes. It's essential for individuals, organizations, and governments to take proactive steps to protect their networks, systems, and data from cyber threats. This includes implementing proper security protocols, staying up-to-date with the latest security patches, and providing employee training on cybersecurity best practices [11].

The following three steps are recommended in order to enhance blockchain security:
When preparing to deploy blockchain technology, offer instruction and training and embrace industry best practices like Gartner's Blockchain Security Model to reduce its dangers. Establish reasonable blockchain regulations and make them global in scope to boost uptake and foster technical confidence.

To handle relevant cybersecurity concerns, minimize risks, and provide ongoing monitoring to new threats and incidents, implement a safe software development practices-based cybersecurity assessment methodology for blockchain systems.

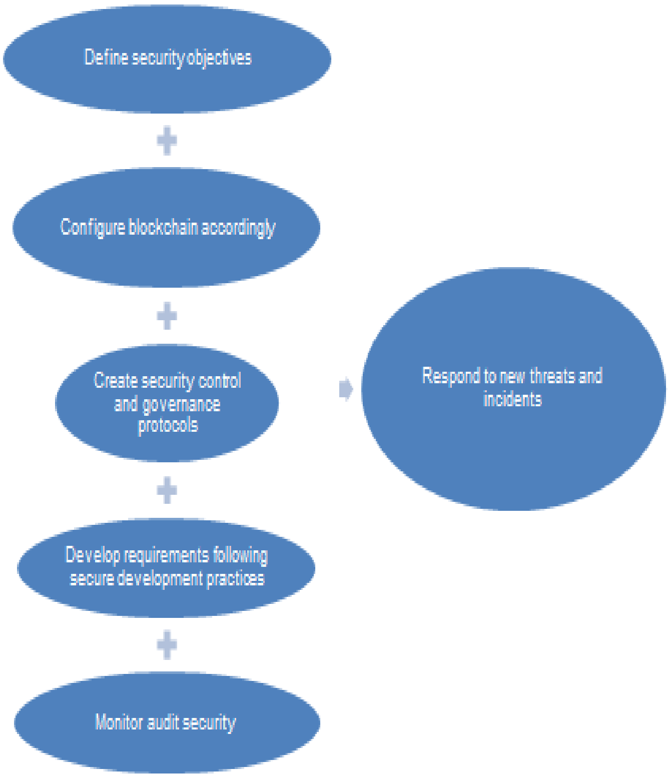
Define security objectives
Configure blockchain accordingly
Create security control and governance protocols
Respond to new threats and incidents
Develop requirements following secure development practices
Monitor audit security

Figure 5. Crucial steps to ensure blockchain security

Determining security objectives that are in line with the present business continuity, crisis management, and security policies is the first step in a suggested procedure, as shown in the figure above. The blockchain system under evaluation needs to be set up to achieve these goals. Stakeholders should then conduct a risk assessment to identify current weaknesses and possible threats. The same paradigm that firms use for other IT deployments may be applied to this assessment as well. In order to lessen the risks that have been recognized, organizations must subsequently implement security controls and related governance procedures. Organizations must create requirements using safe development approaches, such as the secure software development life cycle (S-SDLC) methodology, if software development is necessary. Lastly, in order to respond to fresh threats and occurrences, companies need to regularly monitor and audit security.

Table 1. Cybersecurity Threats with Solution

Cybersecurity Threat	Description	Causes	Solutions
Phishing Attacks	Deceptive emails or messages sent to trick individuals into providing sensitive information	Social engineering tactics; lack of cybersecurity awareness	Educate individuals about the threat of phishing, implement technical solutions such as spam filters and anti-virus software
Malware	Malicious software designed to	Lack of proper cybersecurity protocols or	Install and regularly update anti-

	harm computer systems and networks	user error	virus and anti-malware software on all devices, avoid downloading files or software from untrusted sources, and regularly update all software with the latest security patches
Denial of Service (DoS) Attacks	Attack that floods a network or server with traffic to make it unavailable to users	Lack of proper network security measures or vulnerabilities in network software or hardware	Implement DDoS protection and mitigation solutions, such as firewalls and intrusion detection systems, and monitor network traffic for unusual activity
Advanced Persistent Threats (APTs)	Targeted attacks carried out by skilled attackers using sophisticated techniques	Lack of proper cybersecurity protocols or vulnerabilities in network software or hardware	Implement a multi-layered security strategy, including firewalls, intrusion detection and prevention systems, and data encryption, and conduct regular security audits and vulnerability assessments
Insider Threats	Cybersecurity threats that come from within an organization	Lack of proper security protocols, employee training, or inadequate background checks	Implement security policies and procedures, such as access controls and background checks, and provide employee training and awareness programs
Internet of Things (IoT) Attacks	Attacks on IoT devices that result in data theft, device control, or physical harm to the user	Lack of proper security protocols, vulnerabilities in IoT device software or hardware, or inadequate user training	Implement security measures such as strong passwords, firmware updates, and secure network connections, and regularly monitor IoT devices for unusual activity or unauthorized access
Malware	Malicious software designed to harm computer systems and networks	Lack of proper cybersecurity protocols or user error	Install and regularly update anti-virus and anti-malware software on all devices, avoid downloading files or software from untrusted sources, and regularly update all software with the latest security patches

6. IoT Working Phenomenon with Cybersecurity

The Internet of Things (IoT) refers to the interconnected network of bodily gadgets, motors, domestic appliances, and other gadgets which are embedded with electronics, software program, sensors, and community connectivity, allowing them to accumulate and trade information. IoT gadgets have become increasingly popular in both private and enterprise settings, but their big use has also brought about new cybersecurity dangers and demanding situations. The Internet of Things (IoT) has transformed the way we stay and paintings, permitting us to connect and interact with the world in new and innovative approaches. However, the substantial adoption of IoT gadgets has additionally added new cybersecurity risks and challenges [12].

Another undertaking in securing IoT gadgets is the massive and constantly evolving attack floor. With so many linked devices, there are various entry points for hackers to make the most. Furthermore, many IoT gadgets are deployed in opposed environments or remote places, making them hard to reveal and secure. To deal with those demanding situations, a number of cybersecurity answers have been evolved for IoT gadgets. These solutions variety from basic protection capabilities which include strong passwords and encryption to extra superior measures like intrusion detection and prevention structures and device mastering-based totally anomaly detection.

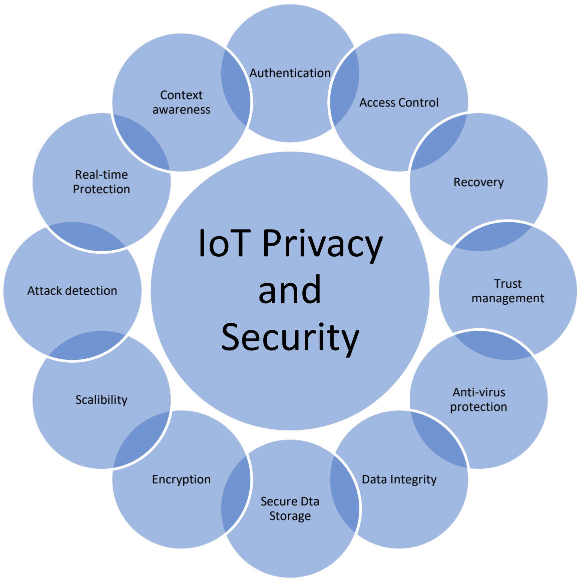

Figure 5. Privacy and security issues in IoT

Analytically, it is important to take a holistic method to IoT security, thinking about not just technical answers, however also organizational tactics and guidelines. For instance, businesses have to put in force threat management practices to pick out capacity vulnerabilities and threats, and establish protocols for incident reaction in case of a protection breach. Finally, ongoing education and education for both give up-customers and IT professionals is crucial to preserving IoT safety. This can consist of training on protection great practices, as well as cognizance campaigns to promote vigilance and caution whilst using IoT devices. In summary, securing IoT gadgets requires a multi-faceted method that mixes technical solutions, organizational guidelines, and person training. While the demanding situations are considerable, with the right strategies and gear, it is possible to steady IoT gadgets and shield towards cybersecurity threats. In phrases of cybersecurity, IoT devices can pose a chance because of their inherent vulnerabilities, which includes susceptible passwords, outdated software, and unsecured verbal exchange channels. Hackers can take advantage of those vulnerabilities to gain get admission to to sensitive records or maybe take manipulate of the devices themselves [13].

To mitigate those risks, it is important to put into effect strong security measures within the design, deployment, and management of IoT devices. This includes:

- ➢ Implementing robust authentication and access controls to prevent unauthorized get entry to to gadgets and information.
- ➢ Encrypting facts both in transit and at relaxation to shield it from interception or theft.
- ➢ Regularly updating firmware and software program to patch vulnerabilities and connect bugs.
- ➢ Implementing intrusion detection and prevention systems to come across and respond to threats in actual-time.
- ➢ Conducting ordinary protection audits and vulnerability exams to discover and cope with weaknesses in IoT structures.
- ➢ Providing worker education and attention applications to ensure that users are aware of the dangers and excellent practices for the use of IoT devices securely.

Securing IoT gadgets and networks requires a multi-layered approach, combining technical solutions and person training to prevent, hit upon, and respond to cybersecurity threats.

Here's a table showing some records on worldwide cyberattacks primarily based on records from exclusive assets. Please observe that those numbers are constantly changing and might range relying at the supply and methodology of facts collection.

Table 2. Records on worldwide cyberattacks primarily based on records from exclusive assets

Year	Total Number of Reported Cyberattacks	Top Cybersecurity Threats
2021	4.83 billion	Malware, phishing, ransomware, DDoS attacks
2020	3.8 billion	Malware, phishing, ransomware, DDoS attacks
2019	3.5 billion	Malware, phishing, ransomware, web-based attacks
2018	2.8 billion	Malware, phishing, web-based attacks, DDoS attacks
2017	1.9 billion	Malware, phishing, web-based attacks, ransomware
2021	Microsoft Exchange Server hack	Microsoft Exchange Server
2020	SolarWinds supply chain attack	SolarWinds
2017	WannaCry ransomware attack	Global
2016	Bangladesh Bank heist	Bangladesh Bank
2014	Sony Pictures hack	Sony Pictures

These are just a few examples of the many cyberattacks that have occurred around the world, causing significant damage to organizations and individuals. It's important to note that cyberattacks can take many different forms and can target any type of organization or individual. It's crucial to stay vigilant and take proactive steps to protect against cyber threats.

- ➢ Was this response better or worse?
- ➢ BetterWorseSame
- ➢ Regenerate response

Sources:

- ➢ SonicWall 2021 Cyber Threat Report
- ➢ Cybersecurity Ventures Cybercrime Report 2020
- ➢ RiskBased Security 2019 Year End Data Breach QuickView Report
- ➢ Symantec Internet Security Threat Report 2019
- ➢ Cybersecurity Ventures Cybercrime Report 2017

7. Cybersecurity Based IoT Equation

One equation that is often used to describe cybersecurity in IoT is:

IoT Security = Device Security + Network Security + Cloud Security + Application Security + User Security

This equation highlights the multiple layers of security that are required to ensure the safety and integrity of IoT devices and systems. Each of the five components in the equation represents a different area of security that must be addressed:

- Device security: This refers to the security measures that are built into IoT devices themselves, such as secure boot processes, encryption, and access controls.
- Network security: This refers to the security measures that are in place to protect the network infrastructure that connects IoT devices, such as firewalls, intrusion detection systems, and secure communication protocols.
- Cloud security: This refers to the security measures that are in place to protect the cloud-based services and infrastructure that support IoT systems, such as data encryption, access controls, and regular security audits.
- Application security: This refers to the security measures that are in place to protect the software applications that are used to control and manage IoT devices and systems, such as secure coding practices, vulnerability testing, and regular updates.
- User security: This refers to the security measures that are in place to protect the end users of IoT devices and systems, such as strong passwords, multi-factor authentication, and security awareness training.

By addressing each of these components and ensuring that they are working together effectively, organizations can improve the overall security of their IoT systems and mitigate the risks of cyberattacks [14].

7.1 Cybersecurity with IoT based Software

Cybersecurity in the IoT often involves software solutions to protect devices, networks, and data from cyber threats. Here are some examples of cybersecurity IoT software:

1. Endpoint security software: This software is installed on individual IoT devices to protect them from cyber threats. Endpoint security software typically includes features such as antivirus, anti-malware, and firewall protection.
2. Network security software: This software is designed to protect IoT networks from cyber attacks. Network security software includes tools for intrusion detection and prevention, network segmentation, and virtual private networks (VPNs).
3. Identity and access management (IAM) software: IAM software is used to manage user identities and access privileges in the IoT. IAM software includes features such as authentication, authorization, and single sign-on.
4. Security information and event management (SIEM) software: SIEM software is used to monitor and analyze security events and data from IoT devices and networks. SIEM software includes features such as log management, threat intelligence, and analytics.
5. Data encryption software: This software is used to encrypt data in transit and at rest in the IoT. Data encryption software includes tools for symmetric and asymmetric encryption, key management, and digital signatures.
6. Firmware security software: Firmware security software is used to protect IoT devices from firmware-level attacks. Firmware security software includes tools for secure boot, firmware validation, and over-the-air updates.

These are just a few examples of cybersecurity IoT software solutions. As the IoT continues to evolve, new software solutions will be developed to address emerging threats and vulnerabilities [15]’

7.2 IoT with Cybersecurity based Software

Cybersecurity-based IoT software refers to software designed specifically for securing the devices and networks that make up the Internet of Things (IoT). Here are some examples of cybersecurity-based IoT software:

1. Armis: Armis is an agentless security platform designed to protect IoT devices and networks. It uses behavioral analytics and machine learning to identify and mitigate cyber threats in real-time.
2. Zingbox: Zingbox is a cloud-based security platform designed specifically for IoT devices. It uses artificial intelligence to detect and respond to cyber threats, and provides visibility into device behavior and security risks.
3. CyberX: CyberX is an industrial cybersecurity platform designed to protect critical infrastructure and industrial control systems (ICS). It uses behavioral analytics and machine learning to identify and mitigate cyber threats in real-time.
4. Darktrace: Darktrace is an AI-powered cybersecurity platform that uses machine learning and behavioral analytics to detect and respond to cyber threats. It can be used to secure IoT devices and networks, as well as other types of IT infrastructure.
5. Forescout: Forescout is an agentless security platform designed to protect IoT devices and networks. It uses behavioral analytics and machine learning to identify and mitigate cyber threats in real-time, and can be used to secure both IT and operational technology (OT) environments.
6. IoT security platforms: These are comprehensive software platforms that provide end-to-end security for IoT devices and networks. They may include features such as device management, data encryption, identity and access management, network security, and security analytics.
7. Endpoint protection: This software is designed to protect individual IoT devices (endpoints) from cyber attacks. It may include features such as antivirus software, intrusion detection and prevention systems, and firewalls.
8. Network security: This software is designed to protect the networks that connect IoT devices. It may include features such as virtual private networks (VPNs), firewalls, and intrusion detection and prevention systems.

9. Identity and access management: This software is designed to manage the identities of users and devices in the IoT, and to control access to IoT systems and data. It may include features such as multi-factor authentication, identity and access management (IAM) systems, and role-based access control (RBAC) systems.
10. Data encryption: This software is designed to encrypt data transmitted between IoT devices and systems to prevent unauthorized access. It may include features such as encryption algorithms and key management systems.
11. Security analytics: This software is designed to analyze data generated by IoT devices and systems to detect and respond to potential cyber attacks. It may include features such as machine learning algorithms, behavioral analytics, and threat intelligence.
12. ZingBox: This is an AI-powered IoT security platform that uses machine learning algorithms to detect and prevent cyber attacks on IoT devices. It provides real-time visibility into IoT devices and network traffic, and offers threat detection and response capabilities.
13. Armis: This platform uses agentless security to discover and profile IoT devices, assess their risk, and enforce security policies. It provides continuous monitoring and threat detection, and can automatically quarantine compromised devices.
14. Forescout: This platform provides agentless security and control for IoT devices, with real-time visibility and automated threat response capabilities. It can identify and classify devices, enforce security policies, and integrate with other security systems.
15. Trend Micro IoT Security: This platform provides comprehensive security for IoT devices, with features such as intrusion detection and prevention, vulnerability management, and threat intelligence. It uses machine learning to identify and block advanced threats.
16. McAfee IoT Security: This platform provides security solutions for IoT devices and networks, with features such as asset discovery, threat detection, and policy enforcement. It uses behavioral analysis and machine learning to identify and respond to threats.

These are just a few examples of cybersecurity-based IoT software. As the IoT continues to grow and evolve, there will likely be an increasing number of software solutions designed specifically for securing these complex systems from cyber threats.

7.3 Cybersecurity with IoT Platform

A cybersecurity IoT platform is a software solution that provides security solutions specifically for IoT devices and networks. These platforms typically provide a suite of tools and technologies for securing IoT devices, networks, and data. Here are some examples of cybersecurity IoT platforms:

1. Azure Sphere: This platform is designed to secure the entire IoT device lifecycle, from development to deployment to decommissioning. It provides hardware-based security, a secure operating system, and cloud-based security services.
2. AWS IoT: This platform provides a suite of security services for IoT devices, including device authentication and authorization, secure communication, and data encryption. It also provides identity and access management, as well as continuous monitoring and threat detection.
3. IBM Watson IoT Platform: This platform provides security solutions for IoT devices and networks, including device authentication and authorization, data encryption, and secure communication. It also provides continuous monitoring and threat detection, as well as advanced analytics and machine learning capabilities.
4. Cisco IoT Security: This platform provides a suite of security services for IoT devices and networks, including device authentication and authorization, secure communication, and threat detection and response. It also provides network segmentation and access control, as well as integration with other security systems.
5. Siemens MindSphere: This platform provides security solutions for IoT devices and networks, including device authentication and authorization, data encryption, and secure communication. It also provides continuous monitoring and threat detection, as well as advanced analytics and machine learning capabilities.
6. Azure Sphere: This platform from Microsoft provides end-to-end security for IoT devices, from hardware to the cloud. It includes a custom microcontroller, a secure operating system, and cloud-based security services.
7. Cisco IoT Security: This platform provides security for IoT devices and networks, with features such as threat detection and response, network segmentation, and policy enforcement. It uses machine learning and behavioral analysis to identify and respond to threats.
8. IBM Watson IoT Platform: This platform provides security solutions for IoT devices and networks, with features such as identity and access management, data encryption, and threat detection. It uses cognitive computing and machine learning to provide real-time threat analysis.
9. IoTium: This platform provides secure connectivity for IoT devices and networks, with features such as endpoint protection, network segmentation, and data encryption. It uses a zero-trust security model to ensure secure communication between devices and the cloud.
10. Palo Alto Networks IoT Security: This platform provides security solutions for IoT devices and networks, with features such as device profiling, threat detection and response, and policy enforcement. It uses machine learning and behavioral analysis to identify and respond to threats.
11. Kaspersky IoT Security: This platform provides comprehensive security for IoT devices and networks, with features such as vulnerability management, threat detection and response, and network segmentation. It also includes tools for managing and monitoring IoT devices and networks.

These are just a few examples of cybersecurity IoT platforms. As the IoT continues to grow and become more complex, cybersecurity platforms will play an increasingly important role in securing these systems and protecting them from cyber attacks [16].

8. Best IoT Devices with Security

IoT devices have become an essential part of our daily lives, and security is a major concern when it comes to using them. Here are some of the best IoT devices with security [17]:

1. Amazon Echo: The Amazon Echo is a popular voice-controlled smart speaker that includes multiple layers of security, such as encryption, secure boot, and secure software updates. It also includes a physical button to turn off the microphone, ensuring privacy when needed.
2. Google Nest Hub: The Google Nest Hub is a smart display that provides access to Google Assistant, home automation, and multimedia features. It includes a camera and microphone, but provides multiple layers of security, such as encryption and a physical switch to disable the microphone and camera.
3. Ring Video Doorbell: The Ring Video Doorbell is a popular IoT device that provides security features for your front door. It includes a camera, motion sensors, and a two-way audio system, and provides end-to-end encryption and secure cloud storage.
4. August Smart Lock: The August Smart Lock is a secure and convenient IoT device that allows you to lock and unlock your door with your smartphone. It uses Bluetooth and Wi-Fi to connect to your phone and includes multiple layers of encryption to ensure security.
5. Arlo Pro 3 Security Camera: The Arlo Pro 3 is a wireless security camera that provides high-quality video and audio recordings, motion detection, and cloud storage. It includes end-to-end encryption and secure cloud storage to ensure privacy and security.
6. Nest Secure: Nest Secure is a home security system that uses IoT devices to monitor your home. It includes a range of security features such as motion detection, door and window sensors, and an alarm system. Nest Secure is designed with security in mind, with features such as encryption, secure communication protocols, and tamper detection.
7. Philips Hue: Philips Hue is a smart lighting system that allows you to control your lights from your smartphone or voice assistant. It includes a range of security features such as end-to-end encryption, secure communication protocols, and regular firmware updates.
8. August Smart Lock: August Smart Lock is a smart lock that allows you to control your locks from your smartphone. It includes a range of security features such as encryption, secure communication protocols, and two-factor authentication.
9. Canary Flex: Canary Flex is a smart security camera that allows you to monitor your home from your smartphone. It includes a range of security features such as motion detection, two-way audio, and encrypted video storage.
10. Samsung SmartThings: Samsung SmartThings is a smart home automation system that allows you to control your smart devices from your smartphone. It includes a range of security features such as end-to-end encryption, secure communication protocols, and regular firmware updates.
11. Apple HomeKit: Apple HomeKit is a smart home platform that includes a range of devices from different manufacturers. It uses encryption and secure authentication to protect user data, and has strict security standards for devices that are certified to work with HomeKit.
12. Arlo Pro 3: The Arlo Pro 3 is a wireless security camera system that allows users to monitor their home from anywhere using a smartphone app. It uses encryption and secure authentication to protect user data, and has features such as motion detection and night vision.

These are just a few examples of IoT devices with security features. When choosing an IoT device, it's important to consider the security features included and ensure that the device has been designed with security in mind [18].

9. Cybersecurity CMD in IoT

CMD (Command Prompt) can be used to perform various cybersecurity tasks in IoT [19]. Here are some examples:

1. Ping: The ping command can be used to test the connectivity of IoT devices. By pinging the IP address or hostname of a device, you can check if it is online and responding to requests.
2. Tracert: The tracert command can be used to trace the path that network packets take to reach an IoT device. This can be useful for identifying any routers or switches that may be causing network connectivity issues.
3. Netstat: The netstat command can be used to view active network connections on an IoT device. This can be helpful for identifying any unauthorized connections or processes that may be using network resources.
4. Ipconfig: The ipconfig command can be used to view the network configuration of an IoT device. This includes the IP address, subnet mask, and default gateway. This information can be helpful for troubleshooting network connectivity issues.
5. Nslookup: The nslookup command can be used to query DNS (Domain Name System) servers for information about a domain or hostname. This can be useful for troubleshooting DNS resolution issues.

It's important to note that using CMD to perform cybersecurity tasks in IoT should only be done by individuals with the necessary technical expertise. Incorrectly entering commands or misconfiguring network settings can result in unintended consequences or security vulnerabilities [19].

10. Conclusion and Future Scope

Cybersecurity in IoT (Internet of Things) refers to the measures and strategies implemented to protect the devices, networks, and facts worried in the IoT ecosystem from unauthorized get entry to, cyber assaults, and different protection threats. IoT devices are often connected to the internet and each other, taking into consideration seamless verbal exchange and information sharing. However, this also creates potential vulnerabilities that may be exploited with the aid of cyber criminals. Examples of security threats in IoT encompass unauthorized get entry to to gadgets or networks, data breaches, malware attacks, and denial-of-service (DoS) attacks. To make certain cybersecurity in IoT, safety features together with encryption, strong authentication protocols, everyday software program updates, and steady community configurations are implemented to prevent and mitigate protection threats. IoT protection also involves teaching users on secure IoT practices and ensuring that gadgets are nicely configured and maintained to limit protection risks. IoT gadgets, such as smart homes, wearables, and industrial systems, are often interconnected and generate big amounts of facts that may be susceptible to cyber assaults. These gadgets may additionally have constrained computing energy, making them more at risk of malware and different kinds of cyber attacks. Cybersecurity in IoT includes enforcing safety features, along with encryption, steady authentication, and ordinary software program updates, to protect IoT gadgets and networks from capability threats. It also includes instructing customers on nice practices for tool safety, which include using sturdy passwords and simplest putting in depended on apps and offerings. To ensure cybersecurity in IoT, a multi-layered method is needed, which incorporates securing the devices themselves, securing the networks they operate on, and securing the information this is transmitted among them. This can contain imposing encryption and authentication protocols, maintaining software program updated with protection patches, and using firewalls and different network security measures. Cybersecurity in IoT is a essential difficulty, because the range of connected devices is growing hastily and cyber attacks on IoT gadgets and networks are getting more frequent and complex. Failure to nicely stable IoT gadgets can bring about critical outcomes which includes information loss, privacy violations, and even physical damage. Cybersecurity in IoT refers back to the measures taken to shield the security and privacy of Internet of Things (IoT) gadgets and the records they gather and transmit. IoT gadgets, together with clever thermostats, home protection structures, and commercial sensors, are linked to the net and often collect touchy facts. This records can encompass personal statistics, financial records, and proprietary business records. Cybersecurity in IoT entails imposing safety capabilities inclusive of encryption, authentication, and get admission to manage to prevent unauthorized get right of entry to, robbery, or manipulation of this information. It also entails regularly updating software and firmware to address protection vulnerabilities and staying vigilant in opposition to emerging threats. With the growing number of IoT devices in use, cybersecurity in IoT is turning into an increasing number of essential to make sure the safety and privacy of users and their records. Cybersecurity in IoT (Internet of Things) refers to the protection of net-linked gadgets including clever domestic gadgets, wearables, and industrial machinery from unauthorized get right of entry to, robbery, and damage. With the growing wide variety of gadgets related to the net, the hazard of cyber attacks focused on these gadgets has additionally grown. The cybersecurity in IoT targets to save you assaults which includes records theft, unauthorized get admission to, and tampering with linked gadgets by means of implementing security features together with encryption, stable authentication, and ordinary software updates. The purpose is to make sure the confidentiality, integrity, and availability of statistics and connected gadgets, and to protect them from cyber threats.

Data Availability

The data supporting findings of this study are all presented in the article.

Conflict of Interest

The authors declare no conflicts of interest.

Funding Source

There is no funding source for this paper.

Authors' Contributions

Author-1, Arun Kumar Singh, researched the literature, collected data and organized the study. Author 2 supervised the preparation of the study and gave final approval of the article for publication.

Acknowledgements

We appreciate and thank the International Journal of Scientific in Research in Computer Science and Engineering (isroset) for their assessment and suggestions to improve visibility and clarity.

References

[1] K. Ashton, 'Internet of Things'. RFID Journal, 22, pp.**97–114, 2009.**

[2] A. Aggarwal, N. Chaubey, K. A. Jani, "A simulation study of malicious activities under various scenarios in Mobile Ad hoc Networks (MANETs)". In Proceedings of the 2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), pp.**827-834, 2013**.

[3] J Gubbi, R Buyya, S Marusic, M Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions" Future Generation Computer Systems, 29(7), pp.**1645–1660, 2013.**

[4] R. Caceres, A. Friday, "Ubicomp systems at 20: Progress, opportunities, and challenges", IEEEPervasive Computing, 11(1), pp.**14–21, 2012.**

[5] M. Darianian, M. P. Michael, "Smart home mobile RFID-based Internet-of-Things systemsand services", In International conference on advanced computer theory and engineering, 2008.ICACTE'08, pp.**116–120, 2008.**

[6] R. Roman, J. Zhou, J. Lopez, "On the features and challenges of security and privacy indistributed internet of things", Computer Networks, 57(10), pp.**2266–2279, 2013.**

[7] T. S. Lo ́pez, D. C. Ranasinghe, M. Harrison, D. McFarlane, "Adding sense to the Internet ofThings", Personal and Ubiquitous Computing, 16(3), pp.**291–308, 2012.**

[8] M. Abomhara, G. M. Køien, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks", Journal of Cyber Security, 4(1), pp.**65-88, 2015**.

[9] A. Furfaro, L. Argento, A. Parise, A. Piccolo, "Using virtual environments for theassessment of cybersecurity issues in IoT scenarios", Simulation Modelling Practiceand Theory, 73, pp.**43-54, 2017.**

[10] X. Huang, P. Craig, H. Lin, H. Z. Yan, "SecIoT: a security framework for theInternet of Things", Security and communication networks, 9(16), pp.**3083-3094, 2016**.

[11] P. Garikapati, K. Balamurugan, T.P. Latchoumi. "K-means partitioning approach to predict the error observations in small datasets" Int. J. Comput. Aided Eng. Technol., 17 (4), pp. 412-430, **2022.**

[12] R. Geetha, T. Thilagam, "A review on the effectiveness of machine learning and deep learning algorithms for cyber security", Arch. Comput. Methods, Eng., 28 (4) (2021), pp.**2861-2879, 2021.**

[13] N. Unnisa A, M. Yerva, K. Mz, "Review on intrusion detection system (IDS) for Network security using machine learning algorithms", International Research Journal on Advanced Science Hub, 4 (3) (2022), pp.**67-74, 2022.**

[14] K. Balamurugan, T.P. Latchoumi, T.P. Ezhilarasi, "Wearables to improve efficiency, productivity, and safety of operations", Smart Manufacturing Technologies For Industry, 4.0, CRC Press (2022), pp.**75-90, 2022.**

[15] V. Gaur, R. Kumar, "Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices", Arabian J. Sci. Eng., 47 (2) (2022), pp.**1353-1374, 2022.**

[16] M.A. Ferrag, O. Friha, L. Maglaras, H. Janicke, L. Shu, "Federated deep learning for cyber security in the internet of things: concepts, applications, and experimental analysis", IEEE Access, 9 (2021), pp.**138509-138542, 2021.**

[17] T.P. Latchoumi, R. Swathi, P. Vidyasri, K. Balamurugan, "Develop new algorithm to improve safety on WMSN in health disease monitoring", 2022 International Mobile and Embedded Technology Conference (MECON), IEEE (2022, March), pp. 357-362, 2022.

[18] J. Thom, N. Thom, S. Sengupta, E. Hand, "Smart recon: Network traffic fingerprinting for IoT device identification", 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), IEEE (2022, January), pp.**72-79, 2022.**

[19] D. Saha, G.N.R. Devi, S. Ponnusamy, J. Pandit, S. Jaiswal, P.K. Bh uyan, "Application of nanotechnology in neural growth support system", 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), IEEE (2022, October), pp.**1-6, 2022.**

AUTHORS PROFILE

Arun Kumar Singh currently working as Head of Computer Science in School of Mathematics and Computer Science, PNG University of Technology, Lae, Papua New Guinea. He received B. E. degree in ECE (2002) from Agra University, Agra, M. Tech. Degree in IT-WCC (2005) from IIIT-Allahabad, Prayagraj, India and PhD degree from SU Meerut, India in 2013. He has published more than 50 research papers in reputed international journals and conferences including IEEE and it's also available online. His main research work focuses on Cybersecurity, AI, Sustainability, IoT and Computational Intelligence. He has 20 years of teaching experience and 15 years of research experience.

Alak Kumar Patra earned his B.E. in Civil Engineering from Jadavpur University, Kolkata in 1999, M.E. in Structural Engineering from IIEST Shibpur in 2012, and Ph.D. in Structural Engineering from IIT Kharagpur in 2018. He is currently working as PG CorseCoordinator and Chairman of Research Development and Engagement Committee, in the School of Civil Engineering (SCE), The Papua New Guinea University of Technology since 2022. He is a life time fellow member (F.I.E) of The Institute of Engineer (India). He has more than 28 years' experience in teaching, research and industries.