Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 110 – 118 | e-ISSN:2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.69

Securing Wireless Communication in Cyber-Physical Systems and the Internet of Things: Addressing Security Challenges

Mr. Vivek D. Patil
Department of Artificial Intelligence & Data Science,
Vishwakarma Institute of Information Technology, Pune - INDIA
vivek.patil@viit.ac.in

Sheetal S. Patil
Department of Computer Engineering,
Bharati Vidyapeeth University, College of Engineering, Pune
sspatil@bvucoep.edu.in

Received: 05 April 2023; Revised: 28 May 2023; Accepted: 19 June 2023

Abstract

Safeguarding wireless communication in cyber-physical systems (CPS) and the Internet of Things (IoT) is important to stop hackers, data breaches, and system interruptions. Multiple security risks can affect these systems because they are linked together and depend on wireless communication methods. This essay looks at the security issues that mobile and internet-connected things (IoT) have and suggests ways to fix them. Two of the biggest problems are keeping data sent over wifi networks private and secure. You can keep data safe from people listening in or changing it by using encryption methods like Advanced Encryption Standard (AES) and Rivest Cipher (RC4). Furthermore, security tools like Public Key Infrastructure (PKI) and Digital Signatures can confirm the authenticity of devices and make sure that contact is safe. An additional problem is that radio communication methods can be attacked with tactics like man-in-the-middle and repeat attacks. You can make CPS and IoT systems safer by using secure methods like Transport Layer Security (TLS) and Secure Shell (SSH). Protecting radio contact is also important to avoid problems caused by denial-of-service (DoS) attacks. Employing intrusion detection systems (IDS) and firewalls can assist in finding and blocking harmful traffic, ensuring that communication stays unbroken. Lastly, protecting radio transmission in CPS and IoT is important to avoid many security risks. The security of CPS and IoT systems can be improved by using encryption methods, identification mechanisms, and safe protocols to keep data private, secure, and accessible.

Keywords

Wireless Communication Security, Cyber-Physical Systems, Internet of Things, Encryption Algorithms, Security Challenges

1. Introduction

The internet of things (IoT) and cyber-physical systems (CPS) have changed how we communicate with the world around us. These linked systems have made it possible to automate, watch in real time, and make decisions based on data in many areas, such as industry, healthcare, and transportation. But the broad use of CPS and IoT devices has caused a lot of security worries, especially about the wireless channels that are used to connect these devices [1]. To stop hackers, data breaches, and system interruptions, it's important to protect radio communication in CPS and IoT. Making sure the privacy and security of data sent over wireless networks is one of the hardest parts of protecting wireless communication in CPS and IoT. Sensitive data is being sent more and more, like personal health data in healthcare systems and private information in business settings. This [2] data needs to be kept safe from being listened to or changed. Advanced Encryption Standard (AES) and Rivest Cipher (RC4) are two encryption methods that can be used to protect data so that only approved devices can read it.

Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 110 – 118 | e-ISSN: 2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.69

Authentication [3] is another important part of keeping radio contact safe in the IoT and CPS. Checking the identities of devices and making sure that only real devices can join to these networks is important because so many of them are linked. Devices can be verified using Public Key Infrastructure (PKI) and Digital Signatures, which protects communication lines and stops people who aren't supposed to be there from getting in. Also, wireless communication methods are open to many attacks, like repeat attacks and man-in-the-middle attacks, which makes CPS and IoT systems [4] very vulnerable to security threats. Using safe methods like Transport Layer Security (TLS) and Secure Shell (SSH) can help protect these systems and make them safer in general. Denial-of-service (DoS) attempts can be stopped by making sure that wireless transmission is always available. Intrusion detection systems (IDS) and filters can help CPS and IoT systems find and stop harmful activity, keeping communication lines open [5]. To protecting radio transmission in CPS and IoT is very important to avoid many security risks. Adding encryption methods, identification systems, and secure protocols to CPS and IoT systems can make them safer and make sure that data is kept private, is correct, and is accessible. Dealing with these security issues is necessary to get the most out of CPS and IoT while lowering the risks that come with using them.

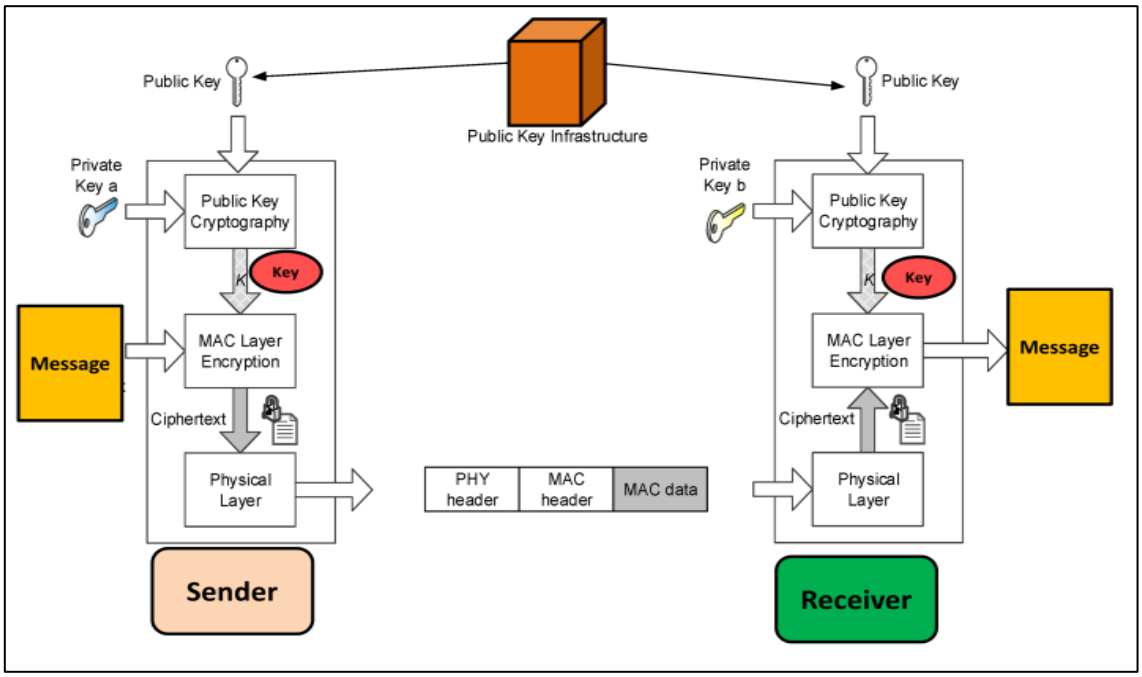

Figure 1: Classical Model of Cryptosystem in cybersecurity

2. Related work

A lot of study has been done on how to keep wireless transmission safe in cyber-physical systems (CPS) and the Internet of Things (IoT). This is because these systems are very important and security breaches could have big effects [6]. A lot of different ideas have been put forward by researchers to help make CPS and IoT devices safer, with a focus on encryption, identification, secure protocols, and attack detection systems. For CPS and IoT, encryption methods are very important for keeping digital contact safe. People use AES a lot because it is very secure and works well to protect data. Researchers have come up with improvements to AES, like Lightweight Cryptography, that would make it easier for IoT devices with limited resources to keep their data safe while still requiring a high level of security. It has been found that RC4, a famous encryption method, can be broken, so it should not be used in safe communication systems anymore [7].

Authentication methods are needed to make sure that devices are who they say they are and that communication routes are safe. PKI is often used to handle digital certificates and make sure that devices in CPS and IoT networks are real. Digital codes are also used to make sure that messages are real and stop people from reading them without permission. In this field of study, the main goal has been to make identification systems more efficient and scalable so they can handle the growing number of devices linked to CPS and IoT networks [8]. Secure methods, [9] like TLS and SSH, are very important for keeping threats

Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 110 – 118 | e-ISSN:2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.69

out of wifi channels. A lot of people use TLS to keep their web communications safe, and it has also been changed to work in CPS and IoT networks. Researchers have come up with lightweight forms of TLS that would keep a high level of security while reducing the load on devices with limited resources. SSH is used to protect access to devices from afar, and it has been improved to allow safe contact in IoT and CPS settings. For CPS [10] and IoT networks to find and stop harmful data, they need intrusion detection systems (IDS) and firewalls. Machine learning-based intrusion detection systems (IDS) have been suggested by researchers as a way to find strange patterns in network data and possible security threats. Firewalls block both incoming and outbound data and keep people from getting into CPS and IoT devices without permission. The main goal of research in this area has been to make IDS and routers that are effective and scalable so that they can keep up with changing security risks.

There has been [11] a lot of work in making radio connection safer in CPS and IoT, but there are still some problems that need to be fixed. One problem is that IoT devices don't have a lot of resources, which makes it hard to add complicated security features. In order to solve this problem while still keeping a high level of security, researchers are looking into lightweight encryption techniques and verification methods. Another problem is that CPS and IoT networks use a lot of different devices and protocols, which can make them hard to connect and leave security holes. Standards and methods that allow different types of gadgets and systems to safely talk to each other are still being researched. It's also hard to handle security in CPS and IoT settings because they are always changing [12]. Adaptive security solutions that can find and stop security risks in real time are being looked into by researchers. These solutions will protect the stability and availability of wireless communication channels. In conclusion, protecting radio transmission in CPS and IoT is a difficult job that needs a number of different approaches. Researchers can improve the safety of CPS and IoT networks and lower the risks of wireless communication by using encryption methods, identification systems, secure protocols, and intruder detection systems. Ongoing study in this area aims to solve the lingering problems and make sure that CPS and IoT systems will work safely and reliably in the future.

Table I: Summary of Related Work

Method	Algorithm	Key Finding	Area	Application	Scope
Lightweight Cryptography	AES	Enhanced AES algorithms reduce computational overhead on resource-constrained IoT devices while maintaining high security levels.	Encryption	IoT Security	Improve efficiency of encryption on IoT
Machine Learning-based IDS	Various ML algorithms	ML-based IDS can detect anomalies in network traffic and identify potential security threats in real-time.	Intrusion Detection	CPS, IoT Networks	Enhance security monitoring capabilities
PKI-based Authentication	RSA, ECC	Public Key Infrastructure (PKI) manages digital certificates and authenticates devices in CPS and IoT networks.	Authentication	CPS, IoT Networks	Improve device identity verification
Lightweight TLS	TLS	Lightweight TLS versions reduce computational overhead on resource-constrained devices while maintaining secure communication channels.	Secure Protocols	CPS, IoT Networks	Enhance efficiency of secure communication
Digital	RSA, DSA,	Digital signatures verify the	Authentication	CPS, IoT	Ensure

Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 110 – 118 | e-ISSN: 2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.69

Signatures	ECDSA	authenticity of messages and prevent unauthorized access to CPS and IoT devices.		Networks	data integrity and secure access
Secure Shell (SSH)	SSH	SSH secures remote access to devices and has been adapted for use in CPS and IoT environments.	Secure Protocols	CPS, IoT Networks	Ensure secure remote device access
Lightweight Encryption	Various algorithms	Lightweight encryption algorithms reduce the computational burden on IoT devices while maintaining data confidentiality and integrity.	Encryption	IoT Security	Improve efficiency of encryption on IoT
Anomaly-based IDS	Various algorithms	Anomaly-based IDS detect deviations from normal network behavior, signalling potential security threats in CPS and IoT networks.	Intrusion Detection	CPS, IoT Networks	Enhance security threat detection
Firewall Protection	Various algorithms	Firewalls filter incoming and outgoing traffic to prevent unauthorized access to CPS and IoT devices.	Network Security	CPS, IoT Networks	Enhance network security
Scalable Authentication	Various methods	Scalable authentication mechanisms accommodate the growing number of devices connected to CPS and IoT networks.	Authentication	CPS, IoT Networks	Improve scalability of authentication
Adaptive Security Solutions	Various methods	Adaptive security solutions detect and respond to security threats in real-time, ensuring the integrity and availability of wireless communication channels.	Security Management	CPS, IoT Networks	Enhance real-time security response
Standard Development	Various standards	Developing standards ensures secure communication between heterogeneous devices and systems in CPS and IoT networks.	Standardization	CPS, IoT Networks	Ensure interoperability and security
Intrusion Prevention Systems	Various methods	IPS prevent security breaches by detecting and blocking malicious traffic in CPS and IoT networks.	Network Security	CPS, IoT Networks	Enhance security threat prevention
Secure Firmware Update	Various methods	Secure firmware update mechanisms ensure that IoT devices receive updates without compromising security.	Firmware Security	IoT Networks	Improve security update process

Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 110 – 118 | e-ISSN: 2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.69

3. Encryption Algorithms for Wireless Communication Security

A. Encryption algorithms

1. AES:

An symmetric encryption method called AES is used to keep data safe when it's sent over wireless channels. A lot of people use it because it works well and is very safe. AES works with blocks of data that are usually 128 bits long. To secure and recover the data, it uses a key. For AES, the key length can be 128, 192, or 256 bits. Keys that are longer are more secure. AES has been studied and reviewed a lot, and it is thought to be very safe against known cipher threats. It's used to keep data safe and private in Wi-Fi (WPA2 encryption) and Bluetooth, among other wireless communication methods. However, AES can be hard to compute, especially on devices with limited resources, which can slow down IoT and CPS apps.

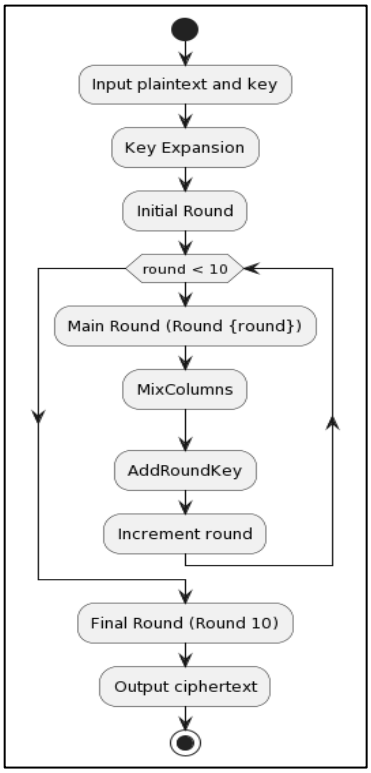

Figure 2: Flowchart of AES

2. Lightweight Cryptography

Lightweight cryptography methods are made to protect devices with limited resources, like IoT devices and sensors, without adding a lot of extra work to the computer. These programs are designed to use memory, computer power, and energy as efficiently as possible. PRESENT, SIMON, and SPECK are all examples of lightweight security methods. These methods are good for radio transmission for CPS and IoT because they strike a good mix between security and speed. These algorithms are made to provide enough security for IoT devices, which may not be able to use traditional algorithms like AES because they need too many resources. When it comes to CPS and IoT, where devices often don't have a lot of computing power, lightweight security methods are very important for keeping radio contact safe. It is possible to get a good amount of protection on these devices without slowing them down by using lightweight methods.

The encryption methods like AES and lightweight cryptography are very important for keeping wireless communication safe in IoT and CPS. Lightweight cryptography methods are better for devices with limited resources than AES, which offers a high level of protection. You can make sure that data sent over wireless channels in CPS and IoT settings is kept private and secure by picking the right encryption method based on the needs of the application.

B. Application of encryption algorithms in securing wireless communication

In Cyber-Physical Systems (CPS) and the Internet of Things (IoT), encryption methods are very important for keeping radio contact safe. These methods are used to keep data sent over wireless networks safe from people who shouldn't be able to see or change it. Encryption is necessary to protect the privacy and security of private data in CPS, which combine physical processes with computing and communication features. Encryption methods are used a lot in CPS and IoT to keep data sent between devices and networks safe. In smart grid systems, for instance, contact between smart meters and the utility company's computers is encrypted to keep it safe. This makes sure that data about how much energy is used is sent safely. Encryption is also used in healthcare systems to protect the privacy of patients when data is sent between medical equipment and electronic health records. Industrial IoT (IIoT) applications also use encryption methods to keep their radio communications safe. Encryption protects contact between sensors, controls, and the central tracking system in factories. This keeps people who aren't supposed to be there from getting in and makes sure that production data is correct.

C. Key findings and advancements in encryption algorithms for CPS and IoT

A lot of important research and progress has been made in encryption methods for CPS and IoT to deal with the

Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 110 – 118 | e-ISSN:2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.69

unique problems these systems present. One important finding is that we need encryption methods that are small and fast, but still provide strong protection. This is especially important for IoT gadgets that don't have a lot of memory or computer power. Because encryption algorithms have gotten better, new algorithms have been made that are especially for IoT and CPS use. For instance, the SIMON and SPECK algorithms are small and fast block ciphers that have been made to work best on Internet of Things (IoT) devices. For IoT and CPS, these methods are perfect for protecting radio transmission because they offer strong security at a low cost.

Another important step forward is the creation of post-quantum encryption methods that are strong enough to withstand attacks from quantum computers. Many encryption methods could be broken by quantum computers, which is a big problem for the safety of IoT and CPS systems. To protect against quantum threats, post-quantum encryption methods like NTRUEncrypt and Lattice-based cryptography are being created.

4. Authentication Mechanisms for Secure Communication

A. Authentication mechanisms

Cyber-Physical Systems (CPS) and the Internet of Things (IoT) need strong authentication methods to make sure that contact is safe. These systems make sure that the devices and people communicating are who they say they are, which stops hackers and data leaks. Public Key Infrastructure (PKI), which verifies devices with digital keys, is a popular way to prove who you are. Each device has a unique certificate that was signed by a trusted source. This lets other devices check that the device is who it says it is. Digital Signatures are another widely used method. They use cryptography to make sure that messages are real. Authentication methods are very important for keeping wireless contact safe in CPS and IoT, where devices often work in places that aren't trusted. These systems help keep bad people from getting into private data or messing with communication lines by making sure devices are who they say they are. Biometric authentication and multi-factor authentication are two examples of new authentication methods that are making radio contact in CPS and IoT even safer. Authentication methods are very important for making sure that contact in CPS and IoT settings is safe and secure.

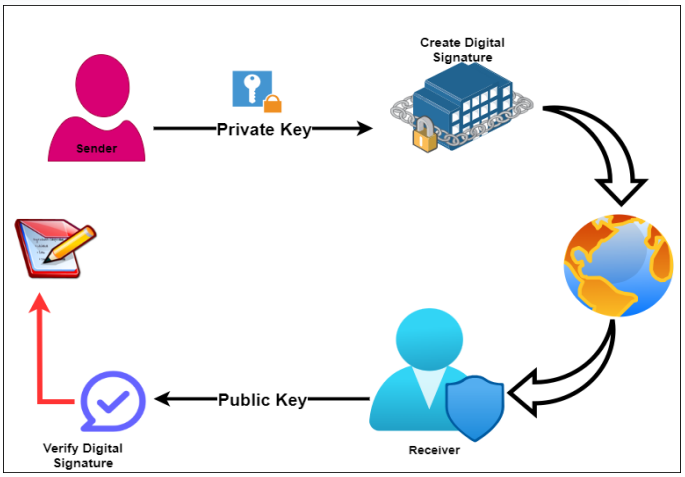

Figure 3: Working of Digital verification

A digital signature is a type of encryption that is used to make sure that a message or document is real and complete. It makes sure that the message came from a known sender and wasn't changed on the way to the recipient. There are two keys used in asymmetric cryptography: a secret key for signing and a public key for checking. This is how digital signatures work.

Algorithm:

1. Key Generation:

- p and q are two big prime numbers. Find their product, n, which is p times q.

$$Find\ \phi(n) = (p-1) \times (q-1).$$

- Choose a number e at random such that 1 is less than or equal to e and that e is coprime to ϕ(n).
- Find d, which is the modular inverse of e modulo ϕ(n).
  This means that $d \times e = 1\ (mod \phi(n))$.
- The private key is (n,d) and the public key is (∃ ,∃) (n, e).

2. signature:

- If you want to sign message m, you need to find
  $$s = m\ d\ (mod n).$$
- s is the signature for message m.

3. Verification

- To check if a signature s is valid for a message m, you need to find
  $$m = s\ e\ (mod n).$$

Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 110 – 118 | e-ISSN: 2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.69

The safety of digital signatures depends on how hard some math problems are, like discrete logarithms or factoring big numbers. The signature method is safe because it is thought to be impossible to compute the private key from the public key and a set of signatures. A lot of private communication methods, like TLS (Transport Layer Security) and PGP (Pretty Good Privacy), use digital fingerprints to make sure that data sent over networks is real and correct.

B. Importance of authentication in securing wireless communication

In Cyber-Physical Systems (CPS) and the Internet of Things (IoT), authentication is a key part of keeping digital contact safe. It makes sure that the people and things communicating are who they say they are, which stops hackers and data leaks. In CPS and IoT settings, where devices often work in dangerous or unsafe situations, authentication is very important. Verifying your name is a key part of identification. Systems can make sure that only approved devices can see private data or use control features by checking the names of devices. In situations like factory robotics, where illegal entry could cause harm or safety risks, this is very important.

Authentication also helps make sure that data sent over wireless networks is correct. By making sure they know who sent the message, receivers can be sure that it hasn't been changed or messed with while it was in transit. This is very important in healthcare systems because patient data needs to be kept safe from people who shouldn't be able to see or change it. Authentication can also help stop man-in-the-middle (MITM) attacks, in which someone listens in on two people's conversation and may change what they say. Systems can find and stop these kinds of scams by making sure that both sides are real. This protects the privacy and security of communication.

C. Implementing authentication mechanisms in CPS and IoT networks

There are a few important steps and things to think about when putting security methods in place in CPS and IoT networks. A popular method is to use Public Key Infrastructure (PKI), which gives devices digital keys that can be used to prove who they are. PSKs are another way to do this. With PSKs, devices share a hidden key that is used for identification. Many objects in CPS and IoT networks don't have a lot of memory or processing power, so verification systems need to be small and quick. Because of this, specially designed identification methods like Lightweight Directory Access Protocol (LDAP) and Remote identification Dial-In User Service (RADIUS) have been made to work well in places with limited resources. Also, identity systems need to be able to grow as the number of objects linked to CPS and IoT networks rises. Because of this, shared identification systems were created so that devices can log in with more than one recognized authority to get to different resources.

D. Challenges and future directions in authentication for CPS and IoT security

Authentication is important for keeping wireless contact safe in CPS and IoT, but there are still some problems to solve. It can be hard to keep track of security keys like digital certificates or PSKs. It gets harder to keep track of these passwords as the number of devices in CPS and IoT networks rises. This problem will need to be fixed in future security systems by making it easier to handle credentials. Another problem is that attacks can be made on login systems. Man-in-the-middle attacks can be used to read verification messages, and brute-force attacks can be used to guess PSKs. To lessen these risks, future authentication systems will need to include strong security features like ongoing authentication and multi-factor authentication. Also, as CPS and IoT networks link to each other more, identification will need to cover more than just devices. It will also need to cover connections between systems and services. Standardized verification methods that can be used in many areas and applications will need to be made in order to do this. Identification is a very important part of keeping digital contact safe in CPS and IoT. Organizations can make sure that their CPS and IoT networks work safely and reliably by tackling the problems and looking into where identification is going in the future.

5. Challenges and Future Directions

A. Limitations of existing security solutions for wireless communication in CPS and IoT

There are some problems with the security methods that are already in place for radio communication in Cyber-Physical Systems (CPS) and the Internet of Things (IoT). One big problem is that security methods and processes are not standardized or able to work with each other. It can be hard to set up safe contact between different settings because different gadgets and systems may use different or private security solutions.

Another problem is that encryption and identification methods may not work well with IoT devices that don't

Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 110 – 118 | e-ISSN: 2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.69

have a lot of resources. Traditional identification and encryption methods may put a lot of extra work on these devices' computers, which could slow them down and drain their batteries faster. Because of this, we need security options that are small, light, and low-power, and that work with IoT devices.

Also, the security solutions we have now might not be able to handle new threats like insider attacks and supply chain weaknesses. Insider attacks, in which approved users take advantage of their access to break security, are a major threat to CPS and IoT systems. Similar to this, supply chain weaknesses, in which harmful parts are added to the chain, can make devices and networks less safe.

B. Emerging threats and vulnerabilities in CPS and IoT environments

A lot of new dangers and weaknesses are making CPS and IoT settings more and more exposed. IoT botnets are becoming more common, which can be used to start large-scale distributed denial-of-service (DDoS) attacks or help people steal data. These botnets use the large number of unprotected IoT devices that are linked to the internet to do bad things.

Another new threat is taking advantage of flaws in the software and hardware that are used in CPS and IoT devices. Attackers can get into devices or change how they work by taking advantage of flaws in the software. Also, flaws in software parts like operating systems and libraries can be used to break into CPS and IoT systems and make them less secure. Also, the fact that CPS and IoT systems are becoming more connected and dependent on each other creates new attack areas and routes. Attackers can use flaws in systems that are linked together to plan joint strikes or get into important assets. This shows how important it is to use security methods that look at the whole ecosystem of gadgets and systems that are linked to each other.

6. Conclusion

Cyber-Physical Systems (CPS) and the Internet of Things (IoT) need a complete method to secure radio communication. This is because the problem is complicated and has many parts. Through this paper, we've talked about how encryption methods, identity systems, and safe protocols are needed to keep data private, secure, and accessible in CPS and IoT settings. It is very important to use encryption methods like AES and lightweight cryptography to send data over wireless networks securely. This keeps private information safe. Authentication tools, like PKI and digital signatures, help make sure that the devices and organizations communicating are who they say they are. This stops people who aren't supposed to be there from getting in and makes sure that the data is correct. Safe contact is made possible by secure methods like TLS and SSH, which stop people from listening in or messing with the messages. Even though encryption techniques and identification methods have come a long way, there are still some problems that need to be solved. Some of these are managing login passwords, making sure that authentication systems are not easy to hack, and the need for uniform security standards. Plus, new threats like IoT botnets and weak spots in the supply chain create new problems that need to be fixed. To make sure that CPS and IoT wireless contact is safer, companies should use a multi-layered security method that includes encryption, identification, secure protocols, and training for employees. To successfully deal with the complicated issues of CPS and IoT security, all parties involved must also work together.

References

[1] K. Khujamatov, E. Reypnazarov, D. Khasanov and N. Akhmedov, "Networking and Computing in Internet of Things and Cyber-Physical Systems," 2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT), Tashkent, Uzbekistan, 2020, pp. 1-6, doi: 10.1109/AICT50176.2020.9368793.

[2] C. Jiang, X. Li, D. Du, L. Wu and R. Findeisen, "Cross-Domain Authentication Scheme Based On Distributed Two-Layer Collaborative Blockchains for Cyber-Physical Power Systems," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2024.3359509.

[3] M. Khalaf, A. Ayad, M. H. K. Tushar, M. Kassouf and D. Kundur, "A Survey on Cyber-Physical Security of Active Distribution Networks in Smart Grids," in IEEE Access, doi: 10.1109/ACCESS.2024.3364362.

[4] A. Bhansali, R. K. Patra, P. B. Divakarachari, P. Falkowski-Gilski, G. Shivakanth and S. N. Patil, "CNN-CLFFA: Support Mobile Edge Computing in Transportation Cyber Physical System," in IEEE Access, vol. 12, pp. 21026-21037, 2024, doi: 10.1109/ACCESS.2024.3361837.

[5] N. Tatipatri and S. L. Arun, "A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security," in

IEEE Access, vol. 12, pp. 18147-18167, 2024, doi: 10.1109/ACCESS.2024.3361039.

[6] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi and R. Ahmad, "Machine learning and deep learning approaches for cybersecuriy: A review", IEEE Access, vol. 10, pp. 19572-19585, 2022.

[7] Ajani, S. N. ., Khobragade, P. ., Dhone, M. ., Ganguly, B. ., Shelke, N. ., & Parati, N. . (2023). Advancements in Computing: Emerging Trends in Computational Science with Next-Generation Computing. International Journal of Intelligent Systems and Applications in Engineering, 12(7s), 546–559

[8] A. Hasankhani, S. M. Hakimi, M. Bisheh-Niasar, M. Shafie-khah and H. Asadolahi, "Blockchain technology in the future smart grids: A comprehensive review and frameworks", Int. J. Electr. Power Energy Syst., vol. 129, Jul. 2021.

[9] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past present and future", Electr. Power Syst. Res., vol. 215, Feb. 2023.

[10] M. Abdalzaher, M. Fouda, A. Emran, Z. Fadlullah and M. Ibrahem, "A survey on key management and authentication approaches in smart metering systems", Energies, vol. 16, no. 5, pp. 2355, Mar. 2023.

[11] Chandu Vaidya, Prashant Khobragade and Ashish Golghate, "Data Leakage Detection and Security in Cloud Computing", GRD JournalsGlobal Research Development Journal for Engineering, vol. 1, no. 12, November 2016.

[12] M. Sewak, S. K. Sahay and H. Rathore, "Deep reinforcement learning in the advanced cybersecurity threat detection and protection", Inf. Syst. Frontiers, vol. 25, pp. 589-611, Aug. 2022.