A REVIEW PAPER ON SECURITY OF IOT SYSTEMS

Kelvin Dmello, Information Science And Engineering, AIET, Karnataka, India

Mr. Pradeep Nayak, Information Science And Engineering, AIET, Karnataka, India

Karthik Madakari T P, Information Science And Engineering, AIET, Karnataka, India

Jahnavi, Information Science And Engineering, AIET, Karnataka, India

Harshitha B, Information Science And Engineering, AIET, Karnataka, India

ABSTRACT

The Internet of Things (IoT) is a significant technology, necessitating businesses to prioritize system security to prevent cyberattacks and system failures. Computer-aided design (CAD) is also advancing, enabling new design revolutions and influencing new research and development directions based on historical and contemporary technology trends. The Internet of Things (IoT) has the potential to significantly change science and engineering systems and daily life. However, it presents challenges such as lower energy and inventory limits, inventory, operations, diversity, ownership, data volume, and attacks. This study reviews these issues and their future possibilities.

Keywords - IoT, CAD, security, predictive maintenance, data integrity, encryption, PPUF, authentication, Industry 4.0

INTRODUCTION

The twenty-first century, known as the age of wireless communication, has seen significant technological advancements in computer networking, including the Internet of Things (IoT), which enables the creation of networks linking digital and physical objects, enabling intelligent sensing and action. Over the past six decades, computer-aided design has evolved from measuring area to energy, reflecting technological advancements.

Speed has become more important than cost, and security indicators have gained attention. Analysis scope has expanded from physical design to logic synthesis, register transfer, behavioural synthesis, and system design. IoT devices and apps are becoming increasingly popular in various industries, including healthcare, where wearable technology is being used to track and share health information. Examples include smart door locks, coffee makers, and smart appliances. Smart city apps include smart street lights, parking, and waste management.

The Internet of Things (IoT) is a rapidly evolving paradigm that allows people and organizations to access and control various devices through the internet. It will significantly change communication and interaction with various services, including learning, health, and resource management.

INTERNET OF THINGS(IOT)

The Internet of Things (IoT) has revolutionized various industries, including smart grids, finance, healthcare, and healthcare. Its predictive maintenance, real-time asset tracking, and energy usage monitoring have significantly improved productivity, reduced downtime, and improved supply chain visibility, leading to financial benefits and reduced carbon footprint.

The Internet of Things (IoT) has revolutionized various industries, enhancing energy monitoring, asset tracking, and predictive maintenance, leading to increased output, reduced downtime, and reduced costs and carbon emissions. Scholars use various methods to tackle security issues, but insufficient research provides a comprehensive understanding. Extensive investigation and analysis are needed to identify issues and explore potential solutions.

The IoT industry offers cost savings, productivity gains, and efficiency improvements. However, implementing IoT faces challenges like expensive infrastructure, data security concerns, and specific skills. Industries must assess the benefits and drawbacks of IoT adoption to realize its full potential.

SECURITY REQUIREMENTS IN IOT

Recent surveys highlight the importance of security in technology, with numerous zero-day assaults emerging as a means for attackers to bypass security systems and annoy innocent users.

Information assurance ensures the safety and security of information systems, ensuring their secrecy, verification, integrity, availability, and non-repudiation. It integrates security, detection, and response capabilities for network restoration, particularly relevant in the context of Internet of Things (IoT) systems that combine digital and physical information worlds.

IoT security regulations ensure the safe operation of connected devices and data. They require robust authentication, access control, encryption, and protection against cyberattacks. Data produced by IoT devices must be protected from manipulation and network-based attacks. These regulations ensure privacy, secrecy, and integrity of data.

IOT SECURITY DESIDERATA

The first lesson covers IoT security requirements, addressing linked but incompatible job requirements. The second class desiderata, cost, size, delay, and energy, limit appropriate security solutions due to their impact on various jobs.

The security of data centres and IoT devices is crucial due to the growing number of devices and the need for unique identification. The IoT infrastructure must track objects continuously, especially in densely populated areas, to prevent restricted access or even impossible access.

High bandwidth and low latency IoT sensors require data integrity methods like watermarking and encryption. Ensuring IoT trust is crucial, and recent plans aim to optimize cost and energy by utilizing hardware security primitives and attestation approaches for software and hardware. Operator trust also affects sensors and IoT.

Intel has demonstrated passive RFID can create a WISP network, where devices gather energy from querying devices. However, using hardware-based security primitives could improve resilience and reduce the number of security operations required. This could be beneficial for creating CAD research and Internet of Things systems.

SECURITY OF DATA

This section discusses the security objectives and specifications of IoT security, focusing on Industry 4.0 applications. It highlights the challenges faced by traditional methods in meeting these security requirements, providing context for understanding the challenges faced by IoT devices.

Data security is increasingly recognized as a crucial component of digital security, especially in the emergence of IoT systems. While data secrecy is necessary for IoT data security, accessibility and consistency are more advantageous in industrial settings. Data protection is a key driver behind Industry 4.0 adoption.

Companies are hesitant to implement data-sharing-based techniques due to insufficient evidence on security and safety. This highlights the need for a consistent approach to protect intellectual property. Most IoT data infractions occur within organizations, leading to the creation of cloud-based storage to mitigate attack surfaces.

Data loss mitigation requires four steps: identification, prevention, recording, and notification. Challenges include minimal resource consumption for data security techniques, the need for concealment in sensitive data sharing, and the increasing demand for data security in private IoT services or applications.

Data security is crucial for IoT devices to protect collected and shared information, ensuring safe storage, encryption, authentication, and access limits to prevent unauthorized access and ensure network security, cybersecurity, and data protection.

FUTURE IMPACT OF IOT

The Internet of Things (IoT) is a technology that manages and governs digital data, reducing complexity and enhancing system performance in cyber, transportation, and healthcare systems. It provides a graphical user interface and cloud computing, enabling access from anywhere. Studies on data security focus on privacy and data sharing, potentially posing unresolved problems.

IoT security requires significant development, with ongoing studies and challenges. Key concerns include real-time data analysis, efficient hardware design, and efficient blockchain use. Alternatives include using intelligent algorithms and machine learning, replacing nodes with effective techniques, and improving fog levels using deep learning and AI.

IoT device makers are incorporating security features into their products due to increasing consumer and business awareness, industry labelling, and managing breaches' reputation and public relations costs.

PUBLIC PUF

PPUFs, which enable public key protocols, are highly useful for protecting IoT devices due to their public nature, ability to withstand side-channel and physical attacks, and significantly less energy and space consumption compared to conventional cryptographic methods.

1. XOR Network Delay PPUF:
   Beckmann et al. proposed the first PPUF model for public key cryptography, which includes gate-level feature As like leakage energy and delay. Process variation causes inherent doping concentration variances, affecting transistors' leakage energy and delay, making the key unpredictable and unclonable. Beckmann's PPUF design consists of a gridded network of XOR gates, each with unique physical attributes due to manufacturing variability. Rising edges race over the network, and each gate changes states when a new edge appears, causing multiple transitions and input challenges.
2. Differential PPUF:
   The differential PPUF allows for long simulation times and high accuracy timing, eliminating the need for precise clock manipulation. Its unclonability relies on manufacturing variability's variations in gate delays. The challenge vector is reduced to a single input vector.
3. Device Aging and Matched PPUFs:

The differential PPUF design, which uses device aging to modify the physical characteristics of the PUF, prevents sustained reverse engineering attempts through dynamic reconfiguration. However, this design has a significant time lag between execution and simulation, making it difficult to facilitate public key communication.

The matched PPUF architecture eliminates the need for simulation by providing globally distinct post-fabrication physical PPUFs that can be made similar using a unique matching technique. This method ensures only involved PPUFs become similar, with a small probability of a third spying opponent matching.

AUTHENTICATION

The rise of IoT devices is increasing security risks in enterprises, necessitating the need for data routing systems to send sensitive information. The data generated by IoT networks requires protection, and current security techniques often fail to consider all security objectives. It is crucial to safeguard these data against various attacks and ensure their feasibility.

The Internet of Things (IoT) has unique characteristics such as multi-hop autonomous design, frequent topology changes, short link lives, media access latency, and multiple security risks. Security-conscious routing is crucial for network efficiency, and Kalyani and Chaudhari proposed a safe cross-layer protocol architecture.

Limited energy and computational resources in Internet of Things devices make research on hacking and communication security challenging. To reduce energy waste, application-specific security methods are optimized for speed while maintaining security, such as the Host Identification Protocol.

SECURITY CHALLENGES IN IOT

1. Lack of encryption
   Encryption is crucial for IoT security, but its similarity to traditional computers increases attacks due to hackers' ability to tamper with security algorithms.
2. Insufficient testing and updating
   As the number of IoT devices increases, manufacturers prioritize speed and lack security, making them vulnerable to hackers and other security issues due to inadequate testing and upgrades.
3. Brute forcing and the risk of default passwords
   IoT devices are vulnerable to brute force and password hacking due to weak login credentials, exposing organizations, assets, and sensitive data to potential attacks.
4. IoT Malware and ransomware
   Ransomware, which uses encryption, effectively prevents consumers from accessing their vital data and information across various platforms and devices as the number of devices increases.
5. IoT botnet aiming at cryptocurrency
   IoT botnets can alter data privacy, posing threats to cryptocurrency markets. Blockchain enterprises aim to enhance security, but app development processes are complex.

CONCLUSION

The Internet of Things (IoT) is a widely used technology, necessitating businesses to prioritize system security to prevent cyberattacks and system failures. IoT security teams face challenges in inventory, operations, and data flow, highlighting the importance of data security in network security. The Internet of Things (IoT) is transforming communication and enabling billions of objects to connect. It surpasses personal computers and mobile phones. Optimizing IoT device design involves combining traditional modelling with optimization-intensive CAD techniques.

Recent hardware security primitives address security and energy constraints effectively. The analysis sorted 564 articles into 25 from 2012-2022, based on inclusion and exclusion criteria. The IoT industry has been retaliating by enabling security solutions to protect devices and systems from intrusions and threats, attracting attention from researchers across geographically dispersed countries and interdisciplinary sectors.

REFERENCE

[1] N. Council, "Disruptive civil technologies: Six technologies with potential impacts on us interests out to 2025," in Conference Report CR, 2008.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] A. Juels, "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 381–394, 2006.

[4] J.-P. Vasseur and A. Dunkels, Interconnecting smart objects with IP: The next internet. Morgan Kaufmann, 2010.

[5] Taherdoost, H. Blockchain-Based Internet of Medical Things. Appl. Sci. 2023, 13, 1287.

[6] Thakor, V.A.; Razzaque, M.A.; Khandaker, M.R.A. Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. IEEE Access 2021, 9, 28177–28193.

[7] Mrabet, H.; Belguith, S.; Alhomoud, A.; Jemai, A. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. Sensors 2020, 20, 3625.

[8] Ahmed, M.I.; Kannan, G. Cloud-Based Remote RFID Authentication for Security of Smart Internet of Things Applications. J. Inf. Knowl. Manag. 2021, 20, 2140004.

[9] Irshad, A.; Usman, M.; Chaudhry, S.A.; Bashir, A.K.; Jolfaei, A.; Srivastava, G. Fuzzy-in-the-Loop-Driven Low-Cost and Secure Biometric User Access to Server. IEEE Trans. Reliab. 2020, 70, 1014–1025.