Original Research Article

J. Computing & Int. Systems (2024) 328–341

Journal of Computing and Intelligent Systems

Journal homepage: www.shcpub.edu.in

ISSN: 2456-9496

A COMPREHENSIVE STUDY ON IOT SECURITY ALGORITHMS

R. John wesly#1, A. John Martin #2

Received on 08 JAN 2024, Accepted on 28 JAN 2024

***Abstract* — IoT security encompasses the measures taken to protect IoT devices, networks, and data from unauthorized access and cyber threats. Algorithms play a key role in ensuring the security of IoT systems. Authentication algorithms are employed to verify the identity of devices and users, while key management algorithms handle the secure generation and distribution of encryption keys. Intrusion detection systems and threat monitoring mechanisms leverage algorithms to identify and respond to potential security breaches. This paper provides IoT security challenges and the algorithms used to address the issues and presents up-to-date security solutions. Security algorithms need technological advancement to face the struggles in fields like Smart homes, Industrial automation, Health care, Agriculture, Smart cities, Environments, Wearables, Smart phones, Traffic Monitoring, and Transportation. This comprehensive study is an attempt to provide insight into the security algorithms used in IoT-enabled services and products**

Keywords — Internet of Things, Security, IoT Devices, Algorithms

I INTRODUCTION

[8] The advent of the Internet of Things (IoT) has ushered in a generation of remarkable connectivity and innovation, remodelling the way we live and paintings. The proliferation of interconnected devices, starting from household appliances to vital business structures, has introduced approximately huge advancements in clever homes, commercial automation, healthcare, agriculture, and the improvement of smart cities. While these innovations provide colossal ability for efficiency, comfort, and sustainability, additionally they boost critical worries, especially in phrases of security.

In this context, the studies problem at hand revolves around the imperative want for robust and complete IoT security features. The interconnected nature of gadgets in smart houses, commercial settings, healthcare systems, agricultural practices, and smart cities demands tailor-made safety solutions. Ensuring the confidentiality, integrity, and availability of information transmitted and stored throughout those domain names isn't always only a technological assignment but a vital prerequisite for the great adoption and sustainable growth of IoT programs.

As we explore the literature on IoT protection in precise domains, which includes smart homes, industrial automation, healthcare, agriculture, and smart cities, Environments, Wearables, Smart phones, Traffic Monitoring, and Transportation, it becomes glaring that a one-length-suits

II. REVIEW OF THE LITERATURE

A. Applications of IOT

[1] The Internet of Things (IoT) refers to a network of interconnected devices that can communicate with each other and share data. IoT devices are used in a variety of applications and industries, ranging from home automation and smart cities to healthcare and agriculture. The following sections provide the area of applications and You can see various IoT applications Fig1.0.

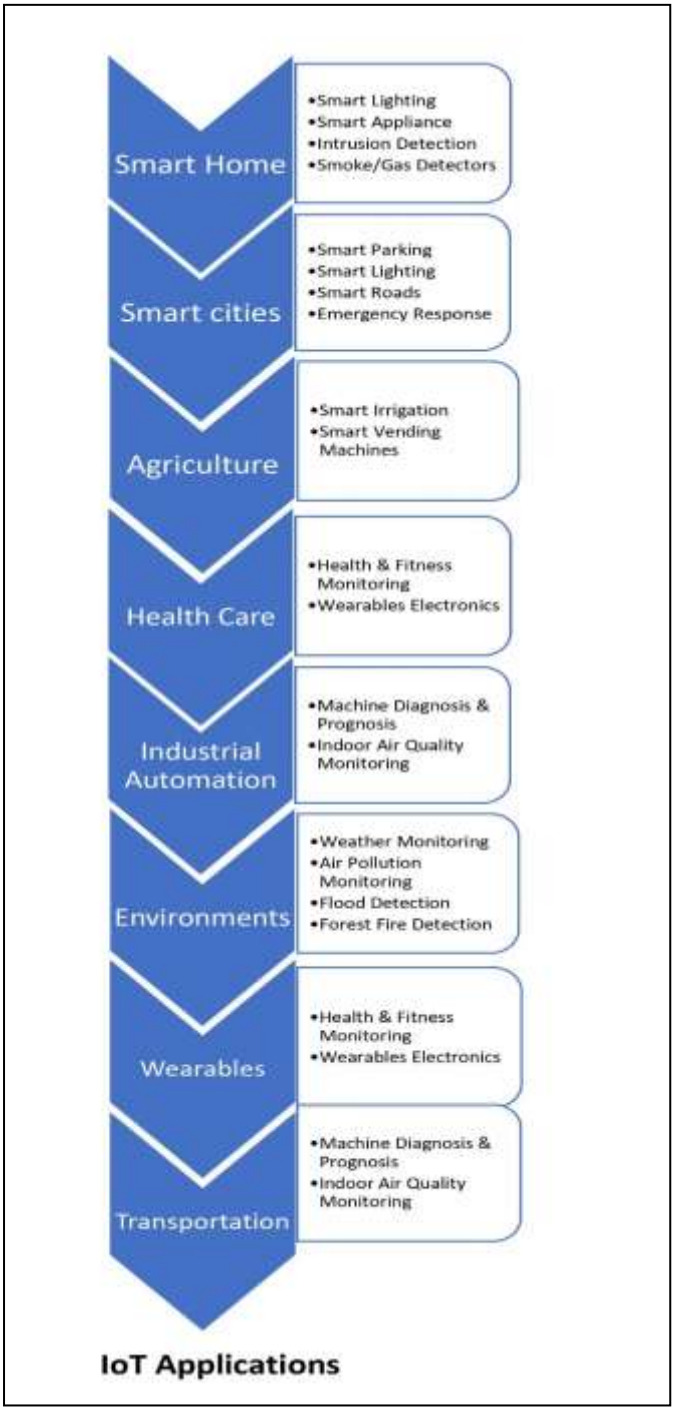
i. Smart Homes

[10] Smart homes are residential that are equipped with smart technologies that can automate and optimize various how use hold functions, such as lighting, heating, ventilation, air conditioning, security, entertainment, and home appliances. These technologies are interconnected through the Internet of Things (IoT), allowing for remote access and control using a mobile device or a computer. Smart homes use sensors, cameras, and other devices to collect data on the home environment and the occupants' behaviour, which can be analysed to provide insights and improve the overall efficiency and comfort of the living space.

*Corresponding author: E-mail: [1]johnweslyr2002@gmail.com, [2]martin@shcpt.edu

[1] MCA Department, Sacred Heart College, Thiruvalluvar University, Tirupattur, Tamil Nadu, India.

[2] MCA Department, Sacred Heart College, Thiruvalluvar University, Tirupattur, Tamil Nadu, India.



While using security algorithms in smart homes can help address security concerns, there are also some challenges to consider. Here are some examples of challenges associated with using security algorithms in smart homes.

a. False alarms: IOT devices such as motion sensors and cameras can be triggered by non-threatening events like pets or moving shadows. This can lead to false alarms, which can be inconvenient and may cause homeowners to ignore future alerts.

b. Privacy concerns: IOT devices collect and transmit data, which can raise privacy concerns for homeowners. Security algorithms that analyse this data could potentially be used to monitor the behaviour and habits of homeowners.

c. Complexity: The domain Smart homes rely on a network of connected devices, which can make them vulnerable to cyber-attacks. Security algorithms must be able to manage the complexity of this network and identify potential security threats.

d. Technical limitations: The IOT devices and the security algorithms may be limited by technical constraints, such as battery life or processing power. This can impact their ability to provide reliable security measures.

e. Compatibility: Smart homes may incorporate devices from different manufacturers, which may not be compatible. This can create challenges when implementing security algorithms that rely on data from multiple devices. These are just a few examples of challenges associated with smart homes, it is important to consider these challenges and implement appropriate measures to mitigate them.

ii. Industrial Automation

handling, and quality control. For example, a factory may use industrial automation to assemble products on an assembly line, where robots and other automated equipment perform tasks such as welding, painting, and packaging. The automation system can monitor and adjust the process in real time, ensuring that products are manufactured to precise specifications. Overall, industrial automation plays an important role in modern manufacturing and industrial processes, helping businesses improve efficiency, quality, and competitiveness in the global marketplace.

While this can increase efficiency and productivity, it also creates potential security challenges for factories. [3] Here are some of the security challenges that factories may face with industrial automation:

a. Cyber security: threats with the increasing use of connected devices and the Internet of Things (IoT) in factories also increase the risk of cyber-attacks. Malware, hacking, and other cyber threats can compromise industrial automation systems and cause significant damage to factories.

b. Insider threats: Employees who have access to industrial automation systems may intentionally or unintentionally cause damage or disruption to the factory. Insider threats can be challenging to detect and prevent, as they may be motivated by various factors such as financial gain or revenge.

c. Physical security: The automation equipment and systems used in factories are often valuable and critical to operations. As such, they may be targeted by thieves or vandals. Physical security measures, such as security

cameras and access control systems, can help prevent unauthorized access and protect automation equipment.

d. Safety risks: Industrial automation systems can pose safety risks if they malfunction or are not properly maintained. Safety hazards may include electrical shocks, explosions, and fires, which can result in injuries or fatalities. Factories must implement proper safety protocols to prevent accidents and ensure the well-being of their employees. As a result, there has been a growing focus on developing security algorithms specifically for industrial automation systems.

iii. Healthcare

The healthcare industry is a major target for cyberattacks, as it stores a vast amount of sensitive patient data. Some of the most pressing healthcare security issues include data breaches, ransomware attacks, phishing attacks, insider threats, and legacy systems. Data breaches occur when hackers gain unauthorized access to sensitive patient data. This data can then be sold on the dark web or used to commit identity theft. Ransomware attacks encrypt a victim's files and demand a ransom payment to restore access. Healthcare organizations are particularly vulnerable to ransomware attacks, as they often have critical data that they cannot afford to lose. Phishing attacks are a type of social engineering attack in which hackers send emails or text messages that appear to be from a legitimate source. These emails or text messages often contain malicious links or attachments that, when clicked, install malware on the victim's computer. Insider threats are posed by employees who have access to sensitive patient data. These employees may intentionally or unintentionally leak data, or they may be tricked by hackers into doing so. Legacy systems are outdated and vulnerable to cyberattacks. These systems are often not equipped with the latest security features, making

them easy targets for hackers. Healthcare organizations need to take steps to protect their data from cyberattacks, such as implementing strong security measures, educating employees about cybersecurity, and backing up data regularly. By taking these steps, healthcare organizations can help protect their patients' data and ensure the safety of their systems. Additionally, cloud usage, mobile devices, and vendor relationships introduce additional risks. Addressing these concerns necessitates a proactive approach, incorporating robust cybersecurity measures, continuous staff training, and close collaboration with experts to safeguard the healthcare ecosystem.

[4] Here are some of the security challenges that factories may face with health care.

a. Masquerade attack: gave a productive, astute middleware game plan (that can be completed in a remote or wired contraption) to support data and system security in medicinal sensor systems.

b. Attacks on wearable and implantable restorative gadgets: proposed two potential safeguards against such assaults.

c. Body-coupled correspondences (BCC): has exhibited a methodology for abusing social connections that exist between individual clients to recognize clone assaults.

d. Accountability and revocability assault: have proposed a strategy that works to recognize and uncover the character of the key abuser.

iv. Agriculture

[15] The agricultural sector is facing a number of security issues, including cyberattacks, natural disasters, pests and diseases, climate change, and food safety. Cyberattacks are a growing threat to the agricultural sector, as they can disrupt operations, steal data, or even release harmful malware. Farmers can protect themselves from cyberattacks by backing up their data regularly, using strong passwords, and being aware of the latest cyber threats.

Natural disasters, such as floods, droughts, and storms, can have a devastating impact on crops and livestock. Farmers can mitigate the risk of natural disasters by investing in weather-resistant infrastructure and crop insurance.

Pests and diseases can also cause significant losses in agricultural production. Farmers can protect their crops from pests and diseases by using pesticides, crop rotation, and other methods. Climate change is already having a negative impact on agriculture, and the effects are expected to worsen in the future. Farmers can adapt to climate change by planting more drought-resistant crops, changing irrigation practices, and using new technologies. Food safety is a critical issue for the agricultural sector, as consumers demand safe and healthy food. Farmers can protect food safety by following good agricultural practices, testing their products for contamination, and keeping their facilities clean.

a. Crop Diseases and Pests: Crop diseases and pests pose a significant threat to agricultural production. Outbreaks can lead to substantial yield losses and financial impact. Managing and mitigating the spread of diseases and pests is crucial for sustainable agriculture.

b. Water Scarcity and Irrigation Management: Water scarcity is a pressing issue in many regions, and agricultural water usage needs to be carefully managed. Efficient irrigation practices and technologies are necessary to optimize water usage and minimize waste.

c. Soil Health and Nutrient Management: Maintaining healthy soil is essential for productive agriculture. Soil degradation, nutrient depletion, and soil erosion pose significant challenges. Proper nutrient management and soil conservation practices are crucial for long-term sustainability.

d. Climate Change and Extreme Weather Events: climate change is impacting agriculture through unpredictable weather patterns, and increased frequency of extreme events such as droughts, and heatwaves. Farmers must adapt to changing conditions, implement climate-resilient practices, and manage risks associated with climate change.

e. Food Safety and Contamination: Ensuring the safety and quality of food products is paramount. Contamination from pathogens, pesticides, or improper handling can have severe health consequences. Proper food safety practices

and traceability systems are critical to maintaining consumer trust.

f. Supply Chain Integrity and Traceability: The complexity of agricultural supply chains introduces vulnerabilities such as fraud, counterfeiting, and product adulteration. Maintaining supply chain integrity and traceability is vital to prevent compromised products from reaching consumers.

g. Data Security and Privacy: As agriculture becomes increasingly digitized, the security and privacy of agricultural data are critical. Protecting sensitive farm data, such as yield records, financial information, and genetic data, from cyber threats and unauthorized access is essential.

h. Rural Infrastructure and Equipment Security: Agricultural operations rely on physical infrastructure and machinery, making them susceptible to theft, vandalism, and unauthorized access. Securing farm equipment, storage facilities, and agricultural infrastructure is crucial for uninterrupted operations.

v. Smarts Cities

Smart cities are urban areas that leverage technology and data to improve the quality of life for their citizens, optimize urban services, and reduce environmental impact. In terms of security, smart cities utilize various technologies, such as CCTV cameras, sensors, and access controls, to monitor and secure public spaces, buildings, and infrastructure. Smart cities rely on a vast network of interconnected devices and systems, making them vulnerable to cyberattacks. These attacks could disrupt critical infrastructure, steal sensitive data, or even cause physical harm. The collection and use of data in smart cities also raise privacy concerns. Governments and businesses may collect large amounts of data about citizens' movements, activities, and preferences. This data could be used for surveillance, marketing, or other purposes without citizens' consent. Additionally, the use of sensors and cameras to monitor public spaces could lead to increased surveillance and the potential for discrimination. There are a number of steps that can be taken to improve the security of smart cities, including implementing strong cybersecurity measures, protecting privacy, and minimizing safety risks. By taking steps to improve security, cities can protect their citizens, their infrastructure, and their economy. [6] The major challenges facing smart cities are urban areas that use advanced technologies and innovative solutions to improve the quality of life face several challenges that must be addressed. Here are some major challenges facing smart cities:

a. Data privacy and security: smart cities rely on the collection and analysis of vast amounts of data from sensors, cameras, and other sources. Ensuring the privacy and security of this data is critical to prevent cyber-attacks and protect citizens' personal information.

b. Digital divide: smart city technologies require reliable high-speed internet connectivity, but many urban areas still lack access to affordable and reliable broadband. This digital divide can lead to unequal access to services and opportunities, exacerbating existing social and economic inequalities.

c. Infrastructure and funding: Implementing smart city technologies requires significant investment in infrastructure, including sensors, communication networks, and data centers. Funding for these initiatives can be difficult to secure, especially for cities with limited budgets.

d. Interoperability and standardization: smart city solutions often come from different vendors and use different technologies, which can make it difficult to integrate them into a cohesive system. Standardization and interoperability are essential to ensure that different systems can communicate and work together seamlessly.

e. Citizen engagement and participation: Smart cities should prioritize citizen engagement and participation to ensure that their needs and preferences are considered in the planning and implementation of new technologies. This requires effective communication and collaboration between government agencies, community organizations, and residents.

f. Environmental sustainability: Smart city technologies can help reduce energy consumption and greenhouse gas emissions, but they can also have negative environmental impacts. Cities must carefully consider the environmental implications of new technologies and prioritize sustainability in their planning and decision-making processes one. This function enables the execution of specific actions or clean-up tasks that are relevant when an activity is not visible. Upon termination of the activity, the on Destroy () function is called.

vi. Environments

[24] Security environments encompass a numerous array of settings wherein facts are saved, processed, or transmitted, every demanding tailored protecting measures. Physically, records facilities and office areas require stringent get admission to controls and surveillance. In the arena of networking, nearby and massive-place networks necessitate firewalls, intrusion detection, and network segmentation. Cloud security mandates careful configuration and get proper of access to manipulate in each public and personal cloud environment. Ensuring endpoint safety entails deploying antivirus software and imposing tool-stage protection policies. The Internet of Things introduces specific demanding situations, requiring strong conversation channels and firmware updates. In virtualized environments, isolation among digital instances is important, necessitating interest to hypervisor and box safety. Application security specializes in safeguarding net and mobile applications towards common vulnerabilities. Compliance with legal and regulatory requirements is important, as is the set-up order and enforcement of security tips during all environments. Security operations centers play a pivotal role in incident response, tracking, and real-time incident detection. In sum, a complete safety approach is vital, addressing physical, virtual, community, and alertness security, along compliance and incident reaction measures to counter evolving threats. The major challenges facing Environments that use advanced technologies and innovative solutions to improve the quality of life face several challenges that must be addressed. Here are some major challenges facing environments:

a. Device Security: Lack of Standardization: The absence of uniform security standards across IoT devices can result in varying levels of security, making it difficult to ensure a consistent and high level of protection.

b. ***Authentication and Authorization:*** The secure and Weak Authentication: Many IoT devices may have weak authentication mechanisms, making them susceptible to unauthorized access. Strong authentication and authorization practices are crucial for preventing unauthorized control or manipulation.

c. ***Data Encryption:*** Insecure Communication: IoT devices often communicate over networks, and if the data is not properly encrypted, it can be intercepted and compromised. Implementing robust encryption protocols is essential for securing data in transit.

d. Device Patching and Updates: Limited Resources: IoT devices often have limited resources, making it challenging to implement regular security updates and patches. This can leave devices vulnerable to known exploits.

e. Physical Security: Device Tampering: Physical access to IoT devices can lead to tampering or unauthorized access. Securing the physical integrity of devices is crucial, especially in applications where physical security is a concern.

f. Network Security: Vulnerable Networks: Inadequate security measures in IoT networks can expose devices to various threats. Network segmentation, firewalls, and intrusion detection systems are essential to secure IoT communications.

vii. Wearables

[25] The proliferation of wearable devices, ranging from smartwatches to fitness trackers, brings forth a host of security considerations that demand careful attention. Wearables, often handling sensitive personal data such as health information and biometrics, necessitate robust measures to safeguard user privacy. Authentication mechanisms and access control on wearables are paramount, particularly as these devices increasingly serve as gateways to various systems. Secure communication protocols and data encryption are essential to protect the integrity and confidentiality of information transmitted by wearables. In healthcare applications, where wearables monitor and transmit critical patient data, additional precautions are needed to prevent unauthorized access and ensure medical data confidentiality. The interoperability of wearables within interconnected ecosystems requires thorough security integration to prevent vulnerabilities. Regular firmware and software updates are crucial to patch vulnerabilities, and manufacturers must comply with regulatory requirements, implementing transparent privacy policies. As wearables often incorporate biometric authentication, protecting this sensitive data through encryption and secure storage is imperative. User awareness and education about security best practices play a pivotal role in mitigating risks associated with wearables, emphasizing the need for strong passwords and an understanding of data-sharing implications.

In navigating the dynamic landscape of wearables, a collaborative effort among manufacturers, developers, and users is essential to establish a secure and privacy-respecting wearable ecosystem. Here are some major challenges facing wearables:

a. Limited Authentication Mechanisms: Wearables often have limited resources, making it challenging to implement robust authentication mechanisms. This limitation can lead to weak password policies or insufficient authentication controls.

b. Biometric Data Security: Many wearables incorporate biometric authentication features, such as fingerprint scanning or heart rate monitoring. Securing biometric data is crucial, as it is sensitive and prone to identity theft if compromised.

c. The Insufficient Encryption Practices: Inadequate encryption of data transmitted between wearables and other devices can expose sensitive information to interception. Ensuring end-to-end encryption is crucial for safeguarding user data.

d. Unauthorized Access via Bluetooth: Wearables often use Bluetooth for communication. Weaknesses in Bluetooth security may allow attackers to gain unauthorized access to wearables, posing a risk to device integrity and user privacy.

e. Lack of Secure Update Mechanisms: Many wearables may lack secure mechanisms for software updates. Without proper update procedures, devices may remain vulnerable to known exploits, putting user data at risk.

f. Data Privacy Concerns: Wearables collect and transmit a wealth of personal data, including health and location information. Ensuring user privacy and securing this data from unauthorized access are ongoing challenges.

viii. Smart phones

[26] Smartphone security features a comprehensive set of measures addressing each hardware and software program aspects to shield consumer records and privateness. Biometric authentication techniques, such as fingerprint scanning and facial popularity, provide steady get entry to, complemented with the aid of strong PINs and passwords. Encryption of saved statistics ensures protection inside the event of theft or loss. Regular running gadget updates are vital to patch vulnerabilities, and app store security performs a pivotal function in vetting and dispensing stable applications. Secure boot tactics and hardware components just like the Trusted Execution Environment contribute to the general safety posture. Network protection, with encrypted connections and cautious use of public Wi-Fi, in addition shields data at some stage in transmission. Two-issue authentication provides a further layer of safety, even as far off tracking and wiping features help mitigate the dangers of tool loss. User schooling about phishing risks, malware safety, and privateness settings enhances normal focus, fostering a greater stable telephone environment. Ultimately, a collaborative attempt concerning customers, producers, and carrier vendors is vital to create a resilient cell protection environment.

Integrating smartphones into the Internet of Things (IoT) ecosystem presents several security challenges that need careful consideration:

a. Interconnected Ecosystem Risks: As smartphones become central hubs in IoT ecosystems, the increased number of connected devices raises the risk of potential

vulnerabilities, providing attackers with more entry points for exploitation.

b. Authentication and Authorization Complexity: Managing authentication and authorization across a diverse range of IoT devices connected to smartphones can be complex. Ensuring secure and seamless access controls is crucial to prevent unauthorized interactions.

c. Data Privacy Concerns: The diverse data collected by IoT devices connected to smartphones, ranging from health metrics to location information, poses significant privacy challenges. Protecting this sensitive information from unauthorized access and misuse is paramount.

d. Insecure Communication Channels: IoT devices often communicate with smartphones through various protocols. Securing these communication channels is essential to prevent eavesdropping, man-in-the-middle attacks, and unauthorized data interception.

e. Device Discovery and Pairing Security: The process of discovering and pairing smartphones with IoT devices introduces security challenges. Ensuring that only authorized devices can connect and communicate is critical to prevent unauthorized access.

f. The Firmware and Software Update Challenges: Coordinating and ensuring the timely update of firmware and software across both smartphones and connected IoT devices is challenging. Outdated software may expose vulnerabilities that can be exploited by attackers.

ix. Traffic monitoring

[28]Traffic monitoring performs a pivotal function in making sure the security of networked systems by using systematically watching and reading records glide. This exercise provides network administrators with crucial visibility into the dynamics of communication, enabling the detection of anomalies and ability safety threats. Utilized for intrusion detection and prevention, site visitors tracking enables discover unauthorized access, malicious sports, and patterns related to malware. Moreover, it aids in enforcing facts loss prevention measures, mitigating denial of service assaults, and carrying out forensic analysis in the aftermath of security incident. As encryption becomes greater widely wide-spread, traffic monitoring faces demanding situations in examining encrypted traffic without compromising privateness, often using answers like SSL/TLS decryption. Beyond reactive measures, site visitors monitoring supports proactive protection techniques, inclusive of user and entity behavior analytics, compliance reporting, and actual-time incident reaction. Its bureaucracy the inspiration for expertise community behavior, improving network segmentation, and leveraging superior technologies like machine getting to know and artificial intelligence to become aware of complex protection styles. In essence, visitors tracking serves as a critical aspect of comprehensive cybersecurity, providing the insights and abilities had to shields the integrity, confidentiality, and availability of networked environments.

Traffic monitoring in the context of the Internet of Things (IoT) introduces specific security challenges that require careful consideration:

a. Heterogeneity of Devices and Protocols: The diversity of IoT devices and the use of various communique protocols pose challenges for visitors tracking. Ensuring compatibility and visibility across different devices and protocols can be complex.

b. Massive Scale and Volume: The sheer scale of IoT deployments and the enormous volume of data generated by connected devices can overwhelm conventional site visitors tracking systems. Scalability becomes a considerable challenge in dealing with the massive amounts of statistics.

c. Encrypted IoT Traffic: Increasingly, IoT devices use encryption to secure information in transit. Monitoring encrypted site visitors for potential threats becomes challenging, as decryption may additionally raise privacy concerns and legal implications.

d. Real-time Processing Requirements: Many IoT programs require real-time processing of data for timely decision-making. Security tracking systems need to keep percent with the fast influx of records to ensure timely threat detection and response.

e. Resource-Constrained IoT Devices: IoT devices often operate with limited computational resources. Implementing security monitoring on resource-constrained devices with out compromising their number one features is a widespread challenge.

f. Device Authentication and Authorization: Ensuring the secure authentication and authorization of IoT devices in the visitors monitoring process is crucial. Unauthorized or compromised devices could potentially manipulate or inject false information into the monitored visitors.

g. Privacy Concerns: IoT devices often collect sensitive records, raising privacy concerns. Balancing the need for security tracking with user privateness expectations and regulatory requirements is a delicate challenge.

h. Data Privacy Concerns: Protecting the privacy of individuals in traffic monitoring systems is a significant challenge. Ensuring that personally identifiable information (PII) is anonymized and securely handled is crucial to comply with privacy regulations.

i. Data Integrity and Authenticity: Verifying the integrity and authenticity of traffic data is essential for preventing manipulation or injection of false information. Ensuring that data collected from various sources is trustworthy is a persistent challenge.

j. Network Security: Securing the communication channels used for transmitting traffic data is critical. Potential threats include eavesdropping, man-in-the-middle attacks, and unauthorized access to the network infrastructure.

k. Denial-of-Service (DoS) Attacks: Traffic monitoring systems are vulnerable to DoS attacks that aim to overwhelm the system with a high volume of requests, disrupting normal operation. Ensuring resilience against such attacks is crucial for maintaining system availability.

x. Transportation

[30]Security in transportation is a complicated and multifaceted enterprise encompassing diverse techniques and technology to ensure the safety and performance of various transportation systems. Physical safety features, together with surveillance cameras, access control, and perimeter safety, are essential components for shielding essential infrastructure such as airports, train stations, and transportation hubs. As technology turns into an increasing number of included into transportation, cybersecurity assumes a pivotal function in protecting related systems, along with GPS, site visitors control, and autonomous cars, towards cyber threats that would compromise passenger safety and disrupt operations. Biometrics and access manipulate technologies enhance airport safety, even as surveillance and monitoring, facilitated by using CCTV systems and superior video analytics, make contributions to situational cognizance. Emergency reaction making plans, shipment security, and border manipulate are critical elements of transportation safety, making sure preparedness, supply chain integrity, and green border crossings. Passenger screening in aviation, security measures in public transit, and steady communications structures are essential for the protection of travelers. Regulatory compliance, resilience making plans, employee schooling, and international cooperation similarly bolster the complete framework required to address evolving protection challenges within the dynamic panorama of transportation. Balancing those measures with privateness considerations guarantees that safety practices align with moral standards and appreciate individual rights. Ultimately, a properly-coordinated and adaptive protection strategy is integral to guard the integrity and capability of transportation systems in an ever-changing protection panorama. Here are key security challenges for transportation in IoT:

a. Device Heterogeneity: The range of IoT devices in transportation, together with sensors, actuators, and communication modules, makes it hard to enforce standardized safety protocols. Ensuring steady security features across numerous devices is a complex mission.

b. Communication Security: The communication among IoT devices in transportation, together with automobile-to-vehicle (V2V) and automobile-to-infrastructure (V2I) communique, must be steady to prevent eavesdropping, tampering, or unauthorized get admission to. Implementing sturdy encryption and authentication is vital.

c. Vulnerabilities in Connected Vehicles: The integration of IoT in linked motors introduces ability vulnerabilities, which includes the danger of unauthorized get admission to to car structures. Protecting cars from cyber threats and ensuring stable firmware updates are vital demanding situations.

d. Data Privacy Concerns: IoT gadgets in transportation generate and exchange giant quantities of data, frequently inclusive of sensitive records. Ensuring the privacy of passenger records and complying with regulations becomes difficult, particularly whilst handling location-primarily based statistics.

e. Scalability and Network Management: Managing safety at scale in massive transportation networks with numerous IoT gadgets is a huge undertaking. Maintaining visibility, monitoring, and manipulate over a big variety of gadgets while ensuring their security poses scalability challenges.

f. Supply Chain Security: The complex deliver chain involved in manufacturing and deploying IoT gadgets for transportation introduces the chance of compromised gadgets. Ensuring the integrity of gadgets for the duration of the supply chain is critical to prevent protection breaches.

Vehicle-to-Everything (V2X) Communication Security: Ensuring secure communication between vehicles, infrastructure, and other entities (V2X) presents challenges such as protecting against eavesdropping, tampering, and replay attacks.

Integrity Verification for Firmware and Software Updates:

Verifying the integrity of firmware and software updates is challenging, particularly in large and diverse fleets of vehicles. Establishing trust in the authenticity of updates is crucial.

Secure Over-the-Air (OTA) Updates: Implementing secure OTA updates without compromising the availability of vehicles is challenging. Balancing the need for frequent updates with the potential impact on operational efficiency is crucial.

Traffic Flow Security: Securing data transmitted within traffic management systems poses challenges related to encryption overhead and real-time processing requirements. Striking a balance between security and system performance is essential.

Connected Infrastructure Security: Securing roadside infrastructure, such as traffic lights and sensors, requires protection against unauthorized access and potential manipulation. Ensuring the security of these interconnected components is crucial for overall system integrity.

III. DISCUSSIONS OF IOT SECURITY AND ALGORITHMS

Table 1. Summary of the Smart Homes Application Algorithm

Ref	Domain	Challenges	Algorithms	Limitations of algorithms
[11]	**Smart Homes**	***A. Clock Synchronization:*** TOTP relies on the accurate synchronization of time between the client device and the authentication server. If there is a time difference between the two, the generated codes will not match, causing authentication failures. ***B. Code Generation Time Window:*** TOTP codes have a limited validity period (usually 30 seconds). If the user doesn't input the code within this window, the code will expire, leading to login delays or failures.	***[13] a. Time-based One-Time Password (TOTP)*** generates a one-time password in a few minutes time to provide a password. ***[13] b. Device Authentication*** algorithms ensure that only authorized devices are allowed to connect to a smart home network. This can include verifying the identity and security posture of devices before allowing them to connect, and requiring that all devices use strong passwords and encryption.	[11] I. The Time-Based One-time password algorithms defect with Network issues because any secret password transformation may often repeat. II. defect and prevent cyber-attacks, such as malware infections and unauthorized access attempts. [18] Intrusion detection systems (IDS) can be used to monitor smart home networks for suspicious activity and alert homeowners or security personnel if an intrusion is detected. It can be helpful.
[7]	**Industrial Automation**	***A. Security Strength:*** Ensuring that encryption algorithms remain secure against various cryptographic attacks, including brute force, cryptanalysis, and quantum computing threats. ***C. Industrial Security Misconfigurations:*** Human error and misconfigurations in access control settings can result in security holes, making it essential to implement proper access control testing and verification procedures.	***[14] a. Encryption algorithms*** can be used to secure communication channels between devices in an industrial automation system. This prevents attackers from intercepting or tampering with sensitive data transmitted between devices. ***[17] b. Access Control*** algorithms ensure that only authorized users have access to the industrial automation system. This can include requiring strong passwords, multi-factor authentication, and role-based access control to limit access to sensitive areas of the system.	***[14] I. Key Management Complexity:*** Encryption requires the use of encryption keys, and managing these keys securely can be challenging, especially in large-scale systems or distributed environments. Key generation, distribution, storage, and rotation all require careful planning and implementation. **[17] II. Misconfigurations Human Errors:** Human error and misconfigurations in access control settings can lead to security vulnerabilities or unintended exposure of sensitive data.

[12]	**Health Care**	***A. Security and Privacy:*** Machine learning models can be vulnerable to adversarial attacks, where carefully crafted inputs can mislead the model's predictions. Ensuring the security and privacy of machine learning systems is a critical challenge. ***B. Data Privacy and Security:*** EHRs contain sensitive patient information, and maintaining data privacy and security is of utmost importance. NLP systems must be designed to comply with strict data protection regulations while allowing access to authorized personnel.	***[8] a. Machine Learning for Diagnosis:*** Machine learning algorithms, such as deep learning and support vector machines, are being used to aid in the diagnosis of various medical conditions. These algorithms can analyze medical imaging data, such as X-rays, MRIs, and CT scans, to assist radiologists and other healthcare professionals in detecting diseases like cancer, neurological disorders, and cardiovascular issues. ***[10] b. NLP for Electronic Health Records (EHRs):*** NLP algorithms are employed to extract valuable information from unstructured text in electronic health records, such as clinical notes and discharge summaries.	***[8] I. Interpretability:*** Many machine learning algorithms, especially deep learning models, are often considered "black boxes" because they lack transparency in how they arrive at specific decisions. The lack of interpretability can be a significant concern, especially in critical medical applications, where doctors and patients need to understand the reasoning behind a diagnosis. ***[10] II. Lack of Standardization:*** EHRs from different healthcare providers may use different coding systems, standards, and formats. The lack of standardization can make it difficult for NLP algorithms to handle the variability in data representation.

Ref	**Domain**	**Challenges**	**Algorithms**	**Limitations of algorithms**
[15]	**Agriculture**	***A. Real-time Detection:*** In agriculture, timely detection is crucial to prevent rapid spread and mitigate damage. Implementing real-time disease and pest detection algorithms requires efficient computational resources and low-latency response times, which can be challenging to achieve in resource-constrained environments. ***B. Scalability:*** Automated harvesting algorithms need to be scalable, enabling them to handle large-scale agricultural operations efficiently.	***[16] a. Disease and Pest Detection:*** Machine learning algorithms are trained on vast datasets of plant diseases and pests to detect early signs of infestation or infection in crops. This early detection enables timely intervention, limiting the spread and impact of diseases and pests. ***[21] b. Automated Harvesting:*** Robotics and computer vision algorithms are utilized to automate harvesting processes for various crops. These technologies can precisely identify ripe fruits or vegetables and perform selective harvesting, reducing waste and the need for manual labor.	***[16] I. Data Quality and Diversity:*** The performance of disease and pest detection algorithms heavily relies on the quality and diversity of the training data. Limited or biased datasets may result in reduced accuracy and generalization capabilities of the algorithm, especially when dealing with rare or emerging diseases. ***[21] II. Delicate Handling:*** Certain crops, such as fruits and vegetables, require gentle handling during harvesting to avoid damage. Designing robotic arms or grippers that can handle these crops delicately is complex and may result in some level of bruising or loss.

[22]	**Smart Cities**	***A. Dynamic Traffic Conditions:*** Traffic patterns can change rapidly due to events like accidents, road closures, or large public gatherings. Algorithms must be capable of adapting to these dynamic conditions and providing real-time adjustments to traffic flow. ***B. Public Participation:*** Encouraging public participation in waste segregation and recycling is crucial for the success of waste management algorithms. Overcoming behavioral barriers and motivating residents to follow waste management guidelines can be challenging.	***[23] a. Traffic Management:*** Smart cities leverage various algorithms for traffic management, such as real-time traffic flow prediction, congestion detection, and dynamic traffic signal control. These algorithms help optimize traffic flow, reduce congestion, and enhance transportation efficiency. ***[22] B Waste Management:*** Optimization algorithms are applied to waste collection routes, aiming to minimize fuel consumption, reduce collection time, and optimize the allocation of resources for waste management service.	***[23] I. Privacy and Security:*** Traffic management systems collect vast amounts of data, including location information from vehicles. Ensuring data privacy and protecting against cyber threats is essential for building public trust in these systems. ***[22] II. Lack of real-time data:*** Many waste management algorithms use historical data or predefined schedules for waste collection and disposal. However, waste generation patterns can vary based on factors like holidays, special events, and population fluctuations. Without real-time data, the algorithms may struggle to adapt to dynamic waste generation scenarios.
[23]	**Environmental**	***Biometric Accuracy and Reliability:*** Biometric access control systems, which use algorithms for fingerprint, retina, or facial recognition, face challenges in achieving high accuracy and reliability. Factors like variations in biometric data due to environmental conditions or changes over time can impact the effectiveness of these algorithms. ***Real-Time Processing:*** Many surveillance applications require real-time processing to respond promptly to security incidents. Developing algorithms that can analyze and respond to data in real-time without sacrificing accuracy is challenging.	***Physical Access Control:*** Keypad PIN Algorithms: Algorithms for PIN verification in access control systems, ensuring secure entry to physical spaces. Biometric Matching Algorithms: For fingerprint, retina, or facial recognition systems used in biometric access control. **Surveillance and Monitoring:** Video Analytics Algorithms: Analytical algorithms used in surveillance systems to detect and analyze activities captured by video cameras. Motion Detection Algorithms: Algorithms that identify movement in a monitored area, triggering alerts for security personnel.	***Physical Access Control:*** Risk of PIN Guessing: Traditional keypad PINs are vulnerable to brute-force attacks, where an attacker systematically tries all possible combinations until the correct one is found. False Positives and False Negatives: Biometric systems can produce false positives (incorrectly accepting an unauthorized user) or false negatives (incorrectly rejecting an authorized user), impacting the system's reliability. Video analytics algorithms and motion detection algorithms may produce false positives (detecting activity that is not a security concern) or false negatives (missing actual security incidents). False alarms can lead to wasted resources, while missed events pose a security risk.

Ref	Domain	Challenges	Algorithms	Limitations of algorithms
[30]	**Wearables**	**Performance Impact Challenge:** Robust encryption algorithms, especially those with high levels of security, can introduce computational overhead. This may impact the performance of wearable devices with limited processing capabilities and energy resources. ***User Convenience vs. Security Challenge:*** Implementing strong authentication measures can sometimes be at odds with user convenience. Striking a balance to ensure both security and a positive user experience is challenging.	***Data Encryption:*** Algorithms processing sensitive user data, such as health information or location data, should implement robust encryption techniques to protect data both in transit and at rest. ***Authentication and Authorization:*** Implement secure authentication mechanisms to ensure that only authorized users can access and interact with wearable devices. Authorization policies should be defined and enforced.	***Key Management Complexity Challenge:*** Effectively managing encryption keys, including generation, distribution, storage, and rotation, introduces complexity. Key management is critical, and any lapses in this process can compromise the security of the encrypted data. ***Biometric Vulnerabilities Challenge***: Biometric authentication, while convenient, is not foolproof. Vulnerabilities include the risk of false positives and the potential for biometric data to be spoofed, raising concerns about the overall reliability of biometric authentication.
[27]	**Smart Phones**	***Privacy Concerns Challenge:*** The collection and storage of biometric data on smartphones raise privacy concerns. Users may be hesitant to provide biometric information due to fears of data misuse or unauthorized access. Striking a balance between security and privacy is challenging. ***Protocol Vulnerabilities Challenge:*** Secure communication protocols, such as TLS or SSL, may have vulnerabilities that could be exploited by attackers. Timely patching and updates are crucial to address identified vulnerabilities and ensure protocol resilience.	***Authentication and Authorization:*** Smartphones act as secure authentication devices, utilizing algorithms for biometric verification or PIN-based authentication. Implementing robust authentication algorithms on smartphones ensures secure access to IoT devices, preventing unauthorized control or manipulation. **Secure Communication Protocols:** This is critical for protecting data transmitted between the smartphone and IoT endpoints. Integration of secure communication algorithms, such as TLS (Transport Layer Security) or SSL (Secure Sockets Layer), enhances the confidentiality and integrity of data in transit within the IoT ecosystem.	***User Privacy Concerns:*** Biometric authentication may raise privacy concerns among users due to the collection and storage of sensitive biometric data. Striking a balance between enhancing security and addressing user privacy concerns is challenging. **Complexity and Resource Intensity:** Implementing and managing secure communication protocols can be resource-intensive, especially on devices with limited processing power and battery capacity. Balancing security with device performance is a constant challenge.
		Dynamic and Evolving Environments: Anomaly detection algorithms may struggle in dynamic and evolving environments where normal patterns of behavior change frequently. Adapting to these changes and distinguishing between	***Anomaly Detection Algorithms:*** Anomaly detection algorithms analyze patterns of network traffic and identify deviations from established baselines. Unusual patterns may indicate potential security threats. These algorithms	***False Positives Limitation:*** Anomaly detection algorithms may produce false positives, flagging normal behavior as anomalous. This can lead to unnecessary alerts and potentially diverting resources to investigate non-threatening events.

[29]	**Traffic Monitoring**	anomalies and evolving normal behavior is a challenge. ***Difficulty in Handling Encrypted Traffic:*** Encrypted traffic poses challenges for IDPS, as it may struggle to inspect the contents of encrypted communication. Attackers can leverage encryption to conceal malicious activities. ***Complexity and False Positives***: Intricate or overly complex IDPS rules may generate false positives. Finding the right balance between accuracy and avoiding unnecessary alerts is challenging.	contribute to the early detection of suspicious activities, such as unusual data volume, unexpected device communication, or irregular access patterns. **Intrusion Detection and Prevention Systems (IDPS):** IDPS algorithms monitor network traffic for signs of malicious activities or security policy violations. They can detect and prevent unauthorized access, attacks, or unusual data transmissions. IDPS algorithms enhance the security of IoT networks by identifying and responding to potential intrusions in real-time.	***False Negatives:*** Limitation: IDPS algorithms may produce false negatives, failing to detect actual security incidents. This can occur when attackers use sophisticated evasion techniques that bypass the detection capabilities of the system. ***Signature-Based Limitations Limitation:*** Some IDPS algorithms rely on signature-based detection, which involves identifying known patterns of malicious activity. This approach may struggle to detect new, previously unseen threats or those that use polymorphic techniques to change their signatures.

Ref	Domain	Challenges	Algorithms	Limitations of algorithms
[32]	**Transportation**	ECC may face challenges in resource-constrained IoT devices due to its computational intensity. Implementing ECC on devices with limited processing power and memory could result in slower performance or increased energy consumption. Ensuring a reliable and secure OTA update process can be challenging, particularly in environments with intermittent connectivity. Addressing potential network interruptions during updates and managing the bandwidth requirements for large updates are significant challenges.	***Vehicle-to-Everything (V2X) Communication Security:*** Elliptic Curve Cryptography (ECC) for secure key exchange and data integrity. ***Integrity Verification for Firmware and Software Updates:*** Code signing using digital signatures. ***Secure Over-the-Air (OTA) Updates:*** Secure OTA update mechanisms with encryption and digital signatures. ***Traffic Flow Security:*** Encryption algorithms for securing data transmitted within traffic management systems.	**Elliptic Curve Cryptography – ECC:** ECC is computationally intensive, and implementing it in resource-constrained IoT devices may impact performance. Additionally, the security of ECC relies on the difficulty of solving certain mathematical problems, and advancements in quantum computing could potentially undermine its effectiveness. ***Secure Over-the-Air (OTA) Updates:*** Secure OTA updates face challenges related to bandwidth constraints and potential network interruptions during the update process. Ensuring a reliable and secure update mechanism without affecting the availability of the device can be challenging.

IV. FUTURE WORK

In the agriculture domain, disease and pest detection algorithms and automated harvesting algorithms in agriculture have great possibilities for the enhancement of addressing security issues. The sensitive data used for detecting diseases and pests requires careful privacy management, and the reliance on technology exposes the system to cyber threats. Ensuring the accuracy of detection algorithms is crucial, and protecting automated harvesting systems from theft and misuse is essential. Ethical, intellectual property and regulatory concerns add complexity. Collaborative efforts involving experts, robust data protection, cybersecurity measures, and education are needed to balance the benefits with security. So, agriculture IoT security systems of disease and pest detecting algorithms and automated harvesting algorithms may be upcoming generations give this solution of advanced algorithms.

V. Conclusion

This paper is a bird eye view of IoT security challenges and which algorithms are used in addressing the issues and presenting up-to-date security solutions. However, it is important to consider IoT devices' security algorithms and limitations, as they can be vulnerable to cyber-attacks. IoT devices can collect data in real-time and enable remote monitoring, allowing businesses to make informed decisions quickly. As IoT continues to evolve and become more integrated into our daily lives, it will be crucial for businesses and individuals to stay informed and adapt to this new technology. Ultimately, the success of IoT will depend on its ability to provide tangible benefits to users while maintaining high levels of security and privacy

REFERENCE

[1] Internet of Things: Applications, security, and privacy: A survey Paul Goyal a, Ashok Kumar Sahoo a, Taren Kumar Sharma a, Pramod K. Singh b Article in Materials Today: Proceedings January 2021.

[2] Security and Privacy in IoT: A Survey Poornima M. Chanal1 Mahabaleshwar S. Kakkasageri1© Springer Science Business Media, LLC, part of Springer Nature 2020

[3] Current research on Internet of Things (IoT) security: A survey Mardini Binti Mohamad Noor, Wan Hasina Hassan 2018 Elsevier B.V. All rights reserved.

[4] Recent Security Trends in Internet of Things: A Comprehensive Survey YASMINE HARBI 1, ZIBOUDA ALIOUAT1, ALLAOUA REFOUFI1, AND SAAD HAROUS 2, (Senior Member, IEEE) Received July 28, 2021, accepted August 5, 2021, date of publication August 9, 2021, date of current version August 19, 2021.

[5] A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis Hicham Market 1,2, Sana Benguet 3, *, Adeb Alhomoud 4 and Abderian Jamia 5.

[6] Survey on IoT Security Faculty of Computing and Information Technology /King Abdul Aziz University, Sameer Saleh Alghamdi, 2 – 11 – 20.

[7] Industrial Automation System K. Madhanamohan! R.K. Praveen*, T.R. Nirmalraja*, H. Goutham*, R Sabarinathan* and A. Logeesan*ISSN 2231-1297, Volume 3, Number 6 (2013), pp. 717-726.

[8] Machine Learning with Health Care Perspective Machine Learning and Healthcare: Machine Learning and Healthcare

[9] The Future of the Internet of Things Article in International Journal of Computers, Communications & Control (IJCCC) · April 2017.

[10] Machine Learning with Health Care Perspective Machine Learning and Healthcare: Machine Learning and Healthcare Book · January 2020.

[11] Smart Home System: A Comprehensive Review Arindom Chakraborty,1 Monirul Islam,1 Fahim Shahriyar,1 Sharnali Islam,2 Hasan U. Zaman,3 and Mehedi Hasan Received 6 August 2022; Revised 9 November 2022; Accepted 15 March 2023; Published 21 March 2023.

[12] Review of Security Issues in E-Healthcare and Solutions Conference Paper October 2016 DOI: 10.1109/HONET.2016.7753433.

[13] A RESEARCH PAPER ON SMART HOME Article · July 2020 International Journal of Engineering Applied Sciences and Technology, 2020 Vol. 5, Issue 3, ISSN No. 2455-2143, Pages 530-532 Published Online July 2020 in IJEAST (http://www.ijeast.com).

[14] Security automation in Information technology Sikender Mohsienuddin Mohammad, Surya Lakshmisri #Department of Information Technology & Wilmington University 419 V ST, APT D, Sacramento, CA 95818.

[15] Issues and challenges in Indian agriculture Jibran, Shahid and Mufti, Azra (2019). Issues and challenges in Indian agriculture. Internat. J. Com. & Bus. Manage, 12(2): 85-88, DOI: 10.15740/HAS/IJCBM/12.2/85-88. Copyright@ 2019: Hind Agri-Horticultural Society.

[16] A Study on the Agriculture Sector and the Problems Associated with it which has an Impact on the Farmers Dr. Sumanta Bhattacharya1, Dr. Heera Lal2, Bhavneet Kaur Sachdev, International Journal of Trend .

[17] Scientific Research and Development (IJTSRD) Volume 5 Issue 6, September-October 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470.
[18] Review in Industrial Automation Udit Mamodiya, Priyanka Sharma Research Scholar, Poornima University Ramchandrapura, Vidhani, Sitapura, Jaipur, India IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676, p-ISSN: 2320-3331, Volume 9, Issue 3 Ver. IV (May – Jun. 2014), PP 33-38 www.iosrjournals.org.
[19] Usage and impact of the internet-of-things-based smart home technology: a quality-of-life perspective Leong Yee Rock1. Farzana Parveen Tajudeen1· Yeong Wai Chung Accepted: 20 October 2022.
[20] Security issues and challenges in a cloud of things-based applications for industrial automation Neeraj Kumar Pandey1, Krishna Kumar2, Gaurav Saini3 · Amit Kumar Mishra4, Accepted: 8 March 2023.
[21] Security Threats and Issues in Automation IoT May 2017 DOI:10.1109/WFCS.2017.7991968, Conference: IEEE International Workshop on Factory Communication Systems - a Conference (WFCS 2017) At Trondheim, Norway.
[22] The future of food and agriculture: Trends and challenges, Food and Agriculture Organization of the United Nations, Rome, 2017.
[23] Environmental security in P2P networks Díaz-Verdejo, J.; García-Teodoro, P.; Maciá-Fernández, G. Dpt. Signal Theory, Telematics & Comm. — CITIC-UGR University of Granada Granada, Spain e-mail: {jedv,pgteodor,gmacia}@ugr.es
[24] Research on Environmental Monitoring System Based on Microservices and Data Mining Yu Liu, Junge Huang*, and Ningqi Lu
College of Urban Construction and Safety Engineering, Shanghai Institute of Technology, 201418 Shanghai, P.R.China.
[25] Security challenges for wearable computing a case study John Lindström Lulea University of Technology, Sweden Centre for Distance-spanning Technology {john.lindstrom@cdt.ltu.se}.
[26] Smartphone Security and Privacy: A Survey on APTs, Sensor-Based Attacks, Side-Channel Attacks, Google Play Attacks, and Defenses Zia Muhammad 1, Zahid Anwar 1, Abdul Rehman Javed 2, Bilal Saleem 3, Sidra Abbas 4 and Thippa Reddy Gadekallu 2,5,6,7,8,.
[27] A Survey on Security for Smartphone Device Article in International Journal of Advanced Computer Science and Applications · April 2016 DOI: 10.14569/IJACSA.2016.070426
[28] Smart Traffic monitoring system Charushila Raskar, Dr. Shikha Nema SNDT University, Mumbai, India Conference Paper · August 2018 DOI: 10.1109/ICGCIoT.2018.8753105.
[29] Enhancing Security and Privacy in Traffic-Monitoring SystemsnArticle in IEEE Pervasive Computing · November 2006 DOI: 10.1109/MPRV.2006.69 · Source: IEEE Xplore.
[30] Wearable Technology Devices Security and Privacy Vulnerability Analysis Article in International Journal of Network Security & Its Applications · May 2016 DOI: 10.5121/ijnsa.2016.8302.
[31] Everything You Wanted to Know About transportation Article in IEEE Consumer Electronics Magazine · July 2016 Saraju P. Mohanty Dept. of Computer Science & Engineering University of North Texas Denton, TX 76203. Email: saraju.mohanty@unt.edu
[32] A Study on the Security Algorithm for Contexts transportation, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2014, Article ID 102051, 8 pages http://dx.doi.org/10.1155/2014/102051