WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# A Survey on Data Breach Resilient Sharing Techniques for IoT Devices

***Rajat Bahadduri[1], Vinay Mali[2], Dr. Pijush Barthakur[3]***

MCA student, MCA student, Associate Professor

Department of MCA, K. L. S. Gogte Institute of Technology, Belagavi, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India

**ABSTRACT:**

The rising use of Internet of Things (IoT) devices, particularly in diverse industries, has engendered significant benefits but has also raised additional issues related to data breaches. Due to the resource restraint (usually less CPU, storage and security features like TPM) nature of those devices, they become a sort of paradise for malicious actors. This quite normal for a scenario where data such as sensor readings, environmental information, and even user behavior may fall into the wrong hands if shared between devices and other entities without adequate protection.

In response to this emergent challenge, this paper provides a survey of IoT-centric data breach resilient data sharing techniques. We'll also dig into techniques such as data anonymization, encryption methods like Attributeed Based Encryption (ABE) and Homomorphic Encryption, and intrusion detection systems (IDS). This paper intends to provide developers and researchers with useful analysis on different approaches of data integrity and privacy in various IoT scenarios - how well they perform, what their limitations are and in which roles they can be applied as IoT continues to grow.

**Index Terms—** IoT, data breach, resilient sharing, cryptography, secure communication, blockchain, security, privacy.

## I. Introduction :

The internet of things or IOT has united the real and digital worlds by creating a tangle of interconnected gadgets that permeate our living areas on one end of the scale there is simple user data such as environmental parameters sensor outputs or even user behaviors hidden among a sea of gadgets from smart washing machines to sweat-sensing wearables or industrial sensors the ease of use automation and personalization of iot are made possible by this data collecting but it also creates a massive attack surface in contrast to typical computing devices internet of things iot devices have very low hardware specifications a small cpu insufficient storage and no security protections that are readily exploited.

The very connectedness that makes the internet of things possible also makes a large surface area vulnerable to attacks vulnerabilities such as obsolete firmware insufficient encryption and insecure communication protocols allow hackers to get into networks steal confidential information and interfere with vital infrastructure a data breach in an iot ecosystem could have disastrous effects possible dangers include illegal entry into residences the falsification of medical information and the interruption of vital services strong data sharing security is vital in the iot environment due to the risks of identity theft privacy violations and the interruption of vital services.


Fig 1: IOT Security Components

[Ref: https://www.linkedin.com/pulse/iot-security-safeguarding-connected-devices-data-from-cyber/]

In order to meet this need this study investigates several strategies for robust data sharing and looks at creative ways to protect privacy and data integrity in the rapidly developing iot environment we explore the domain of secure data sharing strategies encompassing access control mechanisms

secure communication protocols and encryption technologies additionally we look at how blockchain technology protects privacy and data integrity and talk about how machine learning and artificial intelligence might be used to improve internet of things security.

Therefore, a decentralized storage mechanism is needed in the future to significantly improve validity, data transparency, and trust among participants without the need for external assistance. Fortunately, the emergence of Bitcoin and its underlying technology, the Interplanetary File System (IPFS) and the Ethereum blockchain, provides a reliable solution for distributed storage systems. Ethereum is a public, permissionless blockchain. dApps are developed using smart contracts, which are automatically executed activities recorded on the Ethereum blockchain and are the main driver of many innovations. Data is stored independently and decentralized on multiple network nodes, which helps ensure better privacy and data availability. In addition, the problem of single point of failure is largely solved by distributed systems.

This survey aims to provide a comprehensive overview of resilient data sharing techniques for IoT devices, focusing on methods to enhance security and protect against data breaches. We will discuss the implementation of secure access control, the application of robust encryption methods, and the integration of blockchain technology to create a more secure and trustworthy IoT environment. Additionally, we will explore the potential of machine learning and artificial intelligence in identifying and mitigating security threats, thereby enhancing the overall security posture of IoT ecosystems. Through this investigation, we aim to highlight innovative approaches and best practices that can be adopted to ensure the safe and efficient operation of IoT networks.

**Motivation :**

This review is being conducted in order to address the growing concern of data breaches in Internet of Things networks. The potential attack surface grows as IoT devices proliferate, requiring strong methods to protect data. The purpose of this study is to present a thorough analysis of current methods for improving data breach resistance in Internet of Things environments

Moreover, the interconnected nature of IoT ecosystems means that a vulnerability in one device can compromise the entire network. This interconnectedness amplifies the potential impact of security breaches, making it imperative to adopt a holistic approach to IoT security. By understanding and mitigating the risks associated with interconnected IoT devices, we can prevent cascading failures and protect critical infrastructure.

In addition, regulatory pressures and standards are evolving to address IoT security concerns. Governments and industry bodies are increasingly recognizing the need for stringent security requirements for IoT devices. Compliance with these regulations not only ensures legal adherence but also promotes consumer trust and confidence in IoT technologies. This review aims to identify best practices and standards that can help organizations comply with regulatory requirements and enhance their security posture.

## 3. Overview of Data Breach in IoT Devices:

IoT devices are particularly vulnerable to data breaches due to several inherent weaknesses. Many IoT devices have limited processing power and storage capacity, which often results in insufficient built-in security measures. Unlike traditional computers, IoT devices frequently lack robust encryption and are sometimes shipped with outdated firmware, making them easier targets for cyber attackers. Additionally, the vast and diverse array of IoT devices creates a large and complex attack surface. Insecure communication protocols and weak or hardcoded passwords further exacerbate the risk, providing multiple entry points for malicious actors to infiltrate networks.

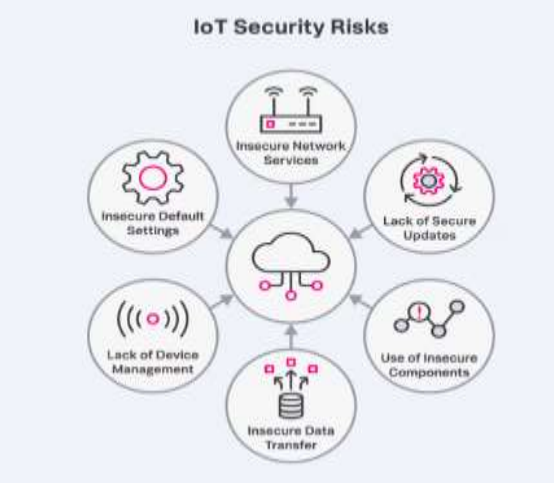


Fig2: IOT Security Risks

[Ref : https://www.splunk.com/en_us/blog/learn/iot-security.html]

The potential consequences of data breaches in IoT contexts are severe and multifaceted. Privacy violations can occur when personal data is accessed or stolen, leading to identity theft and unauthorized surveillance. Financial losses can result from the theft of sensitive financial information or through

disruption of services that require costly repairs or replacements. Safety risks are also a significant concern, especially in critical applications such as healthcare, where tampering with medical devices can endanger patients, or in industrial settings where compromised sensors and control systems can lead to operational failures and accidents.

Moreover, the lack of standardization in IoT security practices contributes to the vulnerability landscape. With the rapid proliferation of IoT devices across various sectors, manufacturers often prioritize functionality and speed to market over security, resulting in devices that are inherently insecure. The heterogeneity of IoT devices—from simple sensors to complex systems—further complicates the implementation of universal security standards. This fragmentation allows attackers to exploit the weakest links in the network, often through a single vulnerable device.

Another critical aspect of IoT data breaches is the challenge of maintaining secure and reliable updates. Many IoT devices lack efficient mechanisms for firmware updates, leading to prolonged periods of vulnerability. Even when updates are available, they may not be applied promptly due to user negligence or lack of awareness. This delay creates an extended window of opportunity for attackers to exploit known vulnerabilities.

The interconnected nature of IoT ecosystems also means that a breach in one device can have cascading effects across the entire network. For instance, an attacker gaining control of a single smart home device can potentially access other connected devices, leading to a broader compromise. In industrial environments, this interconnectedness can result in the disruption of entire production lines, causing significant operational and financial damage.

## 4.Risks in enterprise cloud computing

**Scope:**

The scope of this review encompasses a thorough examination of the diverse methodologies utilized to ensure secure data sharing within IoT networks. The review places particular emphasis on cryptographic techniques, exploring various encryption and decryption methods that safeguard data integrity and confidentiality during transmission and storage.

Additionally, it delves into secure communication protocols, analyzing how they establish and maintain secure channels for data exchange between IoT devices, preventing unauthorized access and data breaches. The scope also includes an exploration of blockchain-based solutions, which leverage distributed ledger technology to enhance the transparency, traceability, and immutability of data transactions in IoT networks.

**Background :**

IoT Architecture

The Internet of Things (IoT) architecture typically comprises three distinct layers: the perception layer, the network layer, and the application layer, each with unique security requirements and potential vulnerabilities.

- Perception Layer : Involves sensors and actuators that collect data.

- Network Layer: Facilitates data transmission between devices.

- Application Layer: Manages data processing and decision-making.

The perception layer, also known as the physical layer, involves the deployment of sensors and actuators that are responsible for collecting data from the physical environment. These devices are often resource-constrained and vulnerable to physical tampering and various cyber-attacks, such as data spoofing and eavesdropping.

The network layer is crucial for facilitating data transmission between IoT devices and systems. It includes both wired and wireless communication technologies, and it is susceptible to a range of threats, including man-in-the-middle attacks, denial of service (DoS) attacks, and unauthorized access. Ensuring secure communication channels and data integrity is vital at this layer.

The application layer is responsible for managing data processing, storage, and decision-making processes.

## 5. Data Breaches in IoT :

Data breaches in IoT networks can arise from several factors, including inadequate authentication mechanisms, unencrypted communication channels, and vulnerabilities within device firmware. These weaknesses can be exploited through various attack vectors, posing significant security risks.

- Man-in-the-Middle (MitM) Attacks : These occur when an attacker intercepts and potentially alters the data being transmitted between IoT devices and their intended recipients. This can lead to unauthorized access to sensitive information and compromise data integrity.

- Distributed Denial of Service (DDoS) Attacks: In these attacks, a network of compromised devices, often referred to as a botnet, is used to flood an IoT system with excessive traffic. This overwhelms the system, leading to disruptions in service availability and potentially causing significant operational downtime.

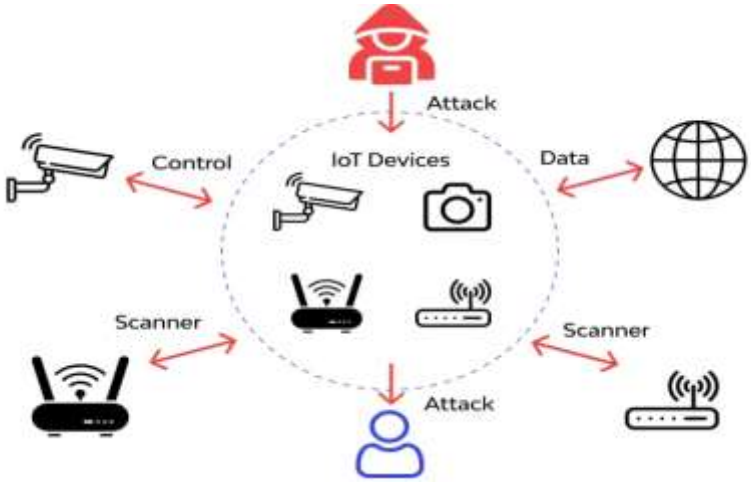


Figure 3 .Challenges in IOT Devices

[Ref : - Firmware Exploits: These involve the exploitation of security vulnerabilities within the firmware of IoT devices. Attackers can manipulate the firmware to gain unauthorized access, control the device, or introduce malicious code,]

- Firmware Exploits: These involve the exploitation of security vulnerabilities within the firmware of IoT devices. Attackers can manipulate the firmware to gain unauthorized access, control the device, or introduce malicious code, thereby compromising the functionality and security of the affected IoT network.

Understanding these common attack vectors is crucial for developing robust security measures to protect IoT ecosystems from potential breaches and ensuring the integrity, confidentiality, and availability of IoT data and services.

Table 1: Summary of IoT Security Incidents in 2023

| Incident | Date | Affected Devices | Impact | Description |
|---|---|---|---|---|
| Smart Home Device Breach | January 2023 | Smart Thermostats, Cameras | Privacy Violation, Unauthorized Access | Hackers exploited weak passwords, gaining access to cameras and thermostats, compromising user privacy. |
| Industrial IoT Attack | March 2023 | Factory Sensors, Controllers | Operational Disruption, Financial Loss | Malware infiltrated factory sensors, causing production halts and significant financial losses. |
| Healthcare Device Breach | May 2023 | Medical Monitoring Devices | Safety Risk, Data Theft | Unauthorized access to patient data and manipulation of medical devices, posing risks to patient safety. |
| Automotive IoT Exploit | August 2023 | Connected Car Systems | Safety Risk, Data Theft | Exploit in connected car systems leading to unauthorized control and theft of user data. |

## 6. Resilient Data Sharing Techniques :

As the Internet of Things (IoT) continues to expand, the security of data shared among interconnected devices becomes increasingly critical. Ensuring data resilience against breaches is paramount to maintaining the integrity, confidentiality, and availability of information in IoT ecosystems. This section explores innovative techniques for resilient data sharing in IoT devices, focusing on methods that enhance security while accommodating the resource constraints typical of IoT environments.

**1. End-to-End Encryption:**

End-to-end encryption (E2EE) ensures that data transmitted between IoT devices remains secure from unauthorized access throughout its journey. By encrypting data at the source and decrypting it only at the destination, E2EE prevents intermediaries from reading or tampering with the data. Lightweight encryption algorithms, such as Elliptic Curve Cryptography (ECC), are particularly suited for IoT devices due to their efficiency and reduced computational overhead.

Upon reaching the healthcare provider's server, only authorized personnel with the decryption keys can access and process the encrypted data. This ensures that intermediaries, such as network providers or unauthorized parties, cannot intercept or tamper with the sensitive health information en route. E2EE thus provides a robust layer of security, maintaining patient confidentiality and compliance with healthcare privacy regulations (such as HIPAA in the United States), while leveraging efficient encryption algorithms suitable for resource-constrained IoT devices.

**2. Secure Communication Protocols :**

Implementing secure communication protocols, such as Datagram Transport Layer Security (DTLS) and Secure MQTT (MQTT-S), is essential for protecting data in transit.

Transport Layer Security (TLS) :

TLS is a widely used protocol designed to secure communications over a network. It ensures that data sent between a client (such as an IoT device) and a server is encrypted, maintaining both data integrity and confidentiality. Consider a smart thermostat in a home automation system. When the thermostat sends data about the current temperature to a cloud server, TLS can be used to encrypt this data during transmission. This prevents anyone from intercepting and reading the data, ensuring that the information remains private and unaltered.

DTLS in Action: Imagine a network of smart sensors monitoring environmental conditions in a remote agricultural field. These sensors use DTLS to securely send data over a less reliable network (like a wireless mesh network) to a central server. DTLS ensures that even if some data packets are lost or arrive out of order, the communication remains secure.

MQTT and CoAP with DTLS

Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) are protocols specifically designed for IoT environments. They are optimized for low-bandwidth, high-latency networks and are lightweight enough to run on resource-constrained devices.

These protocols provide confidentiality, integrity, and authenticity for data exchanges, ensuring that IoT devices communicate securely even over potentially insecure networks. They also support mutual authentication, where both communicating parties verify each other's identity, further enhancing security.

**3. Blockchain and Distributed Ledger Technology :**

Blockchain technology offers a decentralized approach to data sharing, which can significantly improve security and transparency in IoT networks. By using a distributed ledger, data is stored across multiple nodes, making it resistant to tampering and single points of failure. Smart contracts can automate and enforce security policies, while consensus mechanisms like Proof of Stake (PoS) and Directed Acyclic Graphs (DAGs) reduce the computational and energy burdens compared to traditional Proof of Work (PoW) systems.

Supply Chain Management: Consider an IoT-based supply chain system where multiple entities (manufacturers, suppliers, transporters, and retailers) need to share data. Blockchain can be used to manage trust among these parties. Each IoT device (like sensors on shipping containers) records data such as location, temperature, and humidity on the blockchain. Since the blockchain ledger is immutable and decentralized, all parties can trust the data's integrity without needing a central authority. This ensures that the data has not been tampered with, enhancing transparency and security across the supply chain.

Smart Contracts :

Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They automatically enforce and execute predefined rules for data sharing, reducing the risk of unauthorized access and ensuring data is shared only under specific conditions.

**4. Attribute-Based Encryption (ABE) :**

Attribute-Based Encryption (ABE) allows for fine-grained access control in IoT networks. Data is encrypted such that only users with specific attributes or credentials can decrypt it. This method enhances data security by ensuring that only authorized devices or users can access sensitive information. ABE is particularly useful in scenarios where data needs to be shared across diverse and dynamic groups of IoT devices.

In a smart healthcare system, patient data can be encrypted using ABE such that only medical personnel with attributes like "Doctor," "Cardiologist," and "Emergency Access" can decrypt it. This ensures that while doctors and relevant specialists can access critical health information, other personnel without the required attributes cannot, thereby maintaining strict confidentiality and privacy. ABE is particularly useful in scenarios where data needs to be shared across diverse and dynamic groups of IoT devices, ensuring secure and controlled access.

**5. Fog and Edge Computing :**

Fog and edge computing bring processing capabilities closer to IoT devices, reducing latency and enhancing data security. By processing data locally on edge devices or intermediate fog nodes, sensitive information can be analyzed and filtered before being transmitted to the cloud. This approach minimizes the exposure of data to potential breaches during transmission and storage in centralized cloud systems.

Edge devices and fog nodes situated in bank branches or ATMs act as intermediate processing points. They locally analyze transaction data before transmitting it to centralized systems for further processing. For instance, when a customer initiates a transaction at an ATM, edge computing processes

the transaction locally, verifying the user's credentials and checking for anomalies such as potential fraud patterns or account irregularities. Only validated transactions are then forwarded to the bank's central servers, reducing latency and ensuring faster response times. This decentralized approach minimizes the exposure of sensitive financial data to potential breaches during transmission and storage in the cloud. It also enhances overall data security by allowing critical security checks to be performed closer to the point of transaction origination, thereby safeguarding against unauthorized access and cyber threats. Edge and fog computing thus play a crucial role in modernizing banking operations, improving customer experience, and bolstering cybersecurity measures across the financial sector.

**6. Intrusion Detection Systems (IDS) :**

Deploying Intrusion Detection Systems (IDS) tailored for IoT environments can significantly enhance data security. These systems monitor network traffic and device behavior for signs of malicious activity or anomalies. Machine learning algorithms can be used to improve the accuracy and efficiency of IDS, enabling real-time detection and response to potential threats.

Smart Home Security: In a smart home system, various IoT devices like cameras, door locks, and thermostats communicate over a network. A signature-based IDS can monitor this network traffic for patterns that match known malicious activities, such as unauthorized attempts to access the camera feeds or brute-force attacks on smart locks. If the IDS detects traffic that matches a known attack signature, it raises an alert. This method is effective for identifying and mitigating threats that have been previously documented and included in the IDS database.

Anomaly-Based IDS :

Anomaly-based IDS works by establishing a baseline of what is considered normal behavior in the network and then monitoring for deviations from this baseline. This method can detect new, previously unknown attacks by identifying unusual activities.

Industrial IoT System: In an industrial setting, IoT devices like sensors and controllers monitor and control machinery. An anomaly-based IDS can learn the normal operating patterns of these devices, such as regular data transmission rates and typical command sequences. If the IDS detects behavior that deviates significantly from this established baseline—such as an unexpected spike in data transmission from a sensor or unusual command sequences sent to a controller—it flags these as potential threats. This approach is valuable for identifying new types of attacks that do not match any known signatures. However, it may generate false positives if benign anomalies (e.g., maintenance activities) are misinterpreted as threats.

**7. Homomorphic Encryption**

Homomorphic encryption allows computations to be performed on encrypted data without decrypting it first. This technique ensures that data remains secure even during processing, preventing unauthorized access to sensitive information. Although computationally intensive, advancements in lightweight homomorphic encryption schemes are making this approach increasingly viable for IoT applications.

Homomorphic encryption provides a powerful method for ensuring the confidentiality of data shared among IoT devices, especially in contexts where sensitive financial information needs to be securely processed and analyzed. For instance, consider a scenario in which IoT devices are deployed in a smart payment system for retail stores. These devices continuously collect transaction data, including customer payment details such as credit card numbers and transaction amounts.

**8. Secure Boot and Firmware Updates**

Ensuring that IoT devices boot securely and receive authenticated firmware updates is crucial for maintaining data integrity and security. Secure boot processes verify the authenticity and integrity of the device firmware during startup, preventing the execution of malicious code. Additionally, encrypted and signed firmware updates protect against tampering and unauthorized modifications.

Secure boot processes implemented on each IoT device verify the integrity and authenticity of the firmware upon startup. Before any data transmission or processing begins, the device checks cryptographic signatures and hashes to ensure that only genuine and unaltered firmware is executed. This prevents malicious actors from injecting unauthorized code or compromising the device's operational integrity.

Secure boot and authenticated firmware updates in this manner, IoT devices in smart manufacturing environments can effectively protect confidential production data from unauthorized access, tampering, or interception during both operation and maintenance phases. This approach not only safeguards sensitive industrial information but also ensures continuous operational efficiency and resilience against potential cyber threats.

## 8. Conclusion :

In conclusion, the implementation of data breach resilient sharing techniques is paramount for securing IoT devices amidst growing cybersecurity threats. Through techniques such as end-to-end encryption (E2EE), secure communication protocols, blockchain technology, and attribute-based encryption (ABE), IoT ecosystems can mitigate vulnerabilities and safeguard sensitive data.

E2EE ensures data confidentiality by encrypting information from source to destination, preventing unauthorized access throughout transmission. Secure communication protocols like MQTT-S enhance data security during IoT device interactions, minimizing risks of interception and tampering. Blockchain technology provides a decentralized and immutable ledger for secure data storage and transaction validation, enhancing trust and transparency in IoT environments.

Attribute-based encryption enables fine-grained access control based on user attributes, ensuring only authorized entities can decrypt sensitive data. Together, these techniques address various security challenges in IoT, from confidentiality and integrity to availability and privacy. Moving forward, continuous advancements and integrations of these resilient techniques are crucial to fortifying IoT ecosystems against evolving cyber threats, ensuring robust protection of data and maintaining trust in interconnected systems.

Incorporating artificial intelligence (AI) and machine learning (ML) into IoT security frameworks can significantly bolster threat detection and response capabilities. AI and ML can analyze vast amounts of data to identify anomalous behavior and potential security breaches in real time, providing proactive defense mechanisms. For instance, anomaly detection algorithms can flag unusual patterns that may indicate a security threat, enabling timely intervention before any significant damage occurs.The implementation of multi-factor authentication (MFA) can enhance access security by requiring multiple forms of verification before granting access to sensitive data or systems. This adds an extra layer of security, making it more difficult for unauthorized users to compromise IoT devices.

Another critical aspect is the regular update and patch management for IoT devices. Keeping software and firmware up to date ensures that known vulnerabilities are addressed promptly, reducing the risk of exploitation by cybercriminals. Manufacturers and users must prioritize timely updates to maintain the security integrity of IoT systems.

In summary, while data breach resilient sharing techniques such as E2EE, secure communication protocols, blockchain technology, and ABE form the foundation of IoT security, the integration of AI and ML, MFA, and diligent update practices are equally essential. These comprehensive strategies collectively strengthen IoT ecosystems against evolving cyber threats, ensuring the robust protection of data and maintaining trust in interconnected systems. Continuous research and development in these areas will be crucial in adapting to the dynamic landscape of cybersecurity threats, ultimately achieving a secure and resilient IoT environment.

**9. REFERENCES :**


1. IoT Security, Privacy, Safety and Ethics Hany F. Atlam and Gary B. Wills
2. Safeguarding the Internet of ThingsBeing secure, vigilant, and resilient in the connected Age By Irfan Saif, Sean Peasley, And Arun Perinkolam
3. A Review of Security and Privacy Concerns in the Internet of Things (IoT) Muhammad Aqeel,1 Fahad Ali,2 Muhammad Waseem Iqbal ,1 Toqir A. Rana ,3,4 Muhammad Arif,5 and Md. Rabiul Auwul 6
4. A Survey on Resilience in the IoT: Taxonomy, Classification, and Discussion of Resilience Mechanisms Christian Berger, Philipp Eichhammer, And Hans P. Reiser, University Of Passau Jörg Domaschka, Franz J. Hauck, And Gerhard Habiger, Ulm University
5. A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and ApplicationsNATHALIE TAN YHE HUAN 1,2, (Member, IEEE),AND ZURIATI AHMAD ZUKARNAIN 2, (Member, IEEE)
6. IoT Privacy and Security: Challenges and Solutions Lo'ai Tawalbeh 1,*, Fadi Muheidat 2, Mais Tawalbeh 3 and Muhannad Quwaider3
7. Edge Computing and IoT Data Breaches: Security, Privacy, Trust, and Regulation - David Kolevski School of Computing and Information Technology University of Wollongong Wollongong, NSW 2522, Australia ,Katina Michael School for the Future of Innovation in Society Arizona State University Tempe, AZ 85287 US
8. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management -In Lee
9. ResIoT: An IoT Social Framework Resilient to Malicious Activities -Giancarlo Fortino, Senior Member, IEEE, Fabrizio Messina,
10. Domenico Rosaci, and Giuseppe M. L. SarnDomenico Rosaci, and Giuseppe M. L. Sarn
11. Securing Digital Ledger Technologies-Enabled IoT Devices: Taxonomy, Challenges, and Solutions ANASTASIOS N. BIKOS 1 AND SATHISH A. P. KUMAR 2, (Senior Member, IEEE)
12. **Security in Internet of Things: A Review -NAQASH AZEEM KHAN 1, (Member, IEEE), AZLAN AWANG 1, (Senior Member, IEEE),AND SAMSUL ARIFFIN ABDUL KARIM 2,3**
13. Security in Internet of Things: Issues, Challenges, and Solutions -Hanan Aldowah Universiti Sains Malaysia | USM · School of Management Doctor of Philosophy
14. Internet of Things: Security and Solutions Survey Pintu Kumar Sadhu 1,* , Venkata P. Yanambaka 2 and Ahmed Abdelgawad 1 ,1 College of Science and Engineering, Central Michigan University.
15. Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment -ZIA ULLAH 1, BASIT RAZA 1, HABIB SHAH 2,SHAHZAD KHAN 3, AND ABDUL WAHEED 4
16. Advanced security model for multimedia data sharing in Internet of Things -Shalini Dhar1 Ashish Khare1 Rajani Singh