Received: 4 August 2023 | Revised: 8 September 2023 | Accepted: 21 September 2023 | Published online: 21 September 2023

RESEARCH ARTICLE

Archives of Advanced Engineering Science
2024, Vol. 2(4) 215–223
DOI: 10.47852/bonviewAAES32021480

BON VIEW PUBLISHING

Futuristic Vigilance: Empowering Chipko Movement with Cyber-Savvy IoT to Safeguard Forests

Sriranga Narasimha Gandhi Aryavalli[1],* and G. Hemantha Kumar[1]

[1]*Department of Studies in Computer Science, University of Mysore, India*

Abstract: The Chipko Drive is an emotional representation of peaceable protest and environmental embryonic in the 1970s in India, overcooked a worldwide perception for forest preservation. Orchestrated primarily by rural villagers, particularly women, the movement bravely isolated trees and forests from government-sanctioned cataloging. Despite its historic implication, the menace of unlawful deforestation still casts a serenade, hatched by an alleged land mafia that devastates biodiversity and forest-dependent societies. This research board is on a transformative mission to combat deforestation by introducing an innovative auto-survival model, inventively built upon the substance of the Internet of Things (IoT). With the acceptance of an interdisciplinary tactic, the study went into the unified combination of IoT technologies for real-time monitoring and analysis, empowering the forest department to investigate illegal logging with matchless care. At the heart of the study lies the scrupulous architecture of the IoT system, precisely manufactured through an engineering lens and invigorated with tough security measures. Guided by the Secure by Design thought process, this research investigates the security concerns and vulnerabilities, founding an unassailable citadel to protect forest capitals. Enlightening a novel route for forest conservation, this research foresees a future where technology and environmental stewardship blend, cultivating a supportable and thriving ecosystem. The proposed IoT-driven key stands as a witness to stanch hunt of data and innovation, issuing a resounding call for partnership and further autopsy. With this, it empowers global conservation actions to paragon and sustain our green heritage for cohorts to come.

Keywords: Internet of Things (IoT), secure architecture engineering, deforestation, attack vectors, authentication and authorization, environmental preservation

1. Introduction

The Chipko movement has been originating in the 1970s and is one of its kind of an example of popular environmental involvement and as a projecting environmental conservation movement [1]. It gained global recognition for its peaceful protest against deforestation in the Himalayan county of India. This movement, considered by villagers hugging trees to protect them from being chopped, demonstrates the thoughtful connection between societies and woodlands [2, 3].

The history of deforestation is the upshot of the Sindh–India border conflict in 1963 that generated a rapid growth gush in Uttar Pradesh, particularly in the rural Himalayan regions. During this duration, distant logging corporations seized the opportunity to exploit the newly built inner roads and sought access to the regions' vast forest capitals. Unfortunately, this led to the mishandling of profitable logging processes, resulting in simple environmental penalties such as lower farming yields, soil corrosion, exhausted water capitals, and increased overflowing in the nearby areas. As the rural villagers heavily relied on the forests for nourishment, their inability to manage the lands and admission lumber due to government rules further worsened the environmental [4–6] disaster.

In response to the unhelpful impact of important classification, an inspiration of confidence emerged in the form of the Dasholi Gram Swarajya Sangh (DGSM), founded in 1964 by the unrealistic ecologist and Gandhian social futuristic, Chandi Prasad Bhatt. DGSM, later renamed Dasholi Gram Swarajya Mandal, became a substance for rural empowerment by founding small industries that harnessed local resources sustainably.

In April 1973, the Chipko movement's kernels were spread near Mandal in the upper Alaknanda valley when the villagers were denied access to a limited number of trees for constructing agricultural gears. In a confusing move, the government allotted a much larger plot to a generous goods builder, sparking outrage among the villagers. With their appeals falling on deaf ears, Chandi Prasad Bhatt led them into the forest, retaining a single and powerful method—embracing the trees to physically obstruct the loggers. After days of stubborn objections, the government ultimately conceded, revoking the company's logging permit and granting DGSM the originally requested allotment.

The unqualified success of the Mandal protest urged DGSM laborers, alongside the well-known ecologist Sunderlal Bahuguna, to distribute the Chipko strategies to adjacent villages. One of the

*Corresponding author: Sriranga Narasimha Gandhi Aryavalli, Department of Studies in Computer Science, University of Mysore, India. Email: gandhi.aryavalli@gmail.com

most remarkable demonstrations took place in 1974 near the village of Reni, where over 2,000 trees faced looming chopping. In response, the government bade the male country dweller to a nearby city for compensation, aiming to cover the way for the loggers unopposed. However, it was the women of the village, led by the unconquerable Gaura Devi, who stood their ground and crushed and challenged the loggers with firm willpower. Their resilience forced the loggers to depart, and this iconic event encouraged the state government to launch a study into deforestation in the Alaknanda valley, ultimately leading to a ten-year ban on profitable logging in the area.

As the Chipko movement (shown in Figures 1, 2, and 3) evolved, its protests exceeded single incidents and grew into a comprehensive "Save Himalaya" movement, advocating for the protection of the entire ecosystem of the region. Throughout the 1980s, the movement strengthened its endeavors, contrasting the Tehri dam project on the Bhagirathi River and various mining operations, leading to the closure of at least one limestone quarry. Moreover, a huge reforestation campaign was launched, resulting in the planting of over one million trees.

Figure 1
Chipko movement

In this study, we will investigate the transformative digital and Internet of Things (IoT) [7] way to address the pressing concern of deforestation. By leveraging IoT and its technology, our aim is to facilitate real-time tree monitoring, incident response, and the protection of unethical logging. We will propose and design architecture at the physical layer via sensor-actuated channels and integration of networks to establish a secure system to protect the forests technically. In addition, we will tackle various security challenges on the IoT and propose layer-wise security challenges on the IoT for deriving a proposal for secure architecture [8, 9] and engineering solutions to support the Save Earth instant creativity.

It is a bit challenging to build IoT to fight against deforestation and to protect the forest infrastructure [2]. Conservation of forests in a nonviolent IoT way [8] requires secure deployment of IoT infrastructure against ever-evolving cyberattacks. The technical expertise of the IoT with deforestation helps in conservation [10] and sustainable [11] growth.

Our research objectives are to use the technology of usage of the IoT from theory into practice. We will use sensors and data to transform the theoretical approach to deforestation and microclimates [12].

In the past years, there were theoretical concepts where a protected woodland faces a potential threat. The guards visit the location to find the threats. With our research innovation, the IoT system directly detects the unauthorized presence of woodcutters and loggers through the motion sensors and via analyzing the sound waves. In a fraction, the alerts of these motions and sound waves are being sent to forest guards/authorities, who can remotely access the live feeds from the security operations centers or network operations centers. These feeds help them in empowering instant decision-making—deploying guards or military teams to the precise location to prevent illegal cutting or logging of the forest infrastructure.

Integrating the IoT technology with sensors and actuators and embedding them into the tree that acts as a data point helps in elevating an alert. We shape the research's objectives, methodology, and impact [13].

1.1. Principle of the Chipko movement

The core principle of the Chipko movement is to protect forests and their resources peacefully.

1.2. Capabilities of IoT technology

This research has been founded on the base of protecting the forestry infrastructure using the latest technologies such as IoT. IoT could connect devices via sensors, gather realistic data, and enable them to monitor remotely via the sensor-controlled technology backbone of this research. The concept of interconnected sensors, actuators, devices, and data-driven insights formed a practical framework through which the Chipko movement's principle has been extended and actualized.

The synergy between these important pillars facilitated the importance of forest conservation.

Using IoT sensors and actuators, we collect the feed of real-time data and collate and analyze them into the interconnected ecosystem in a proactive approach to safeguard the forests.

1.3. Historical perspective versus technical advancements

The integration of the IoT is the latest trend in securing forest deforestation, while historically, it was used as the Chipko movement. However, there are difficulties in implementing this in a robust way; without good insights, the integration of sensors via IoT technology for environmental survival and protection is practically difficult [14].

1.4. IoT technology and advancements

IoT and its applications use sensors, actuators, and sensor networks for real-time data collection, analysis, and alerting. These sensors were integrated into the forest ecosystem [15] for safeguarding and protecting the forestry infrastructure.

1.5. Communication and connectivity

IoT uses networking such as Wi-Fi, Zigbee, LoRaWAN, and 5G. These have addressed connectivity challenges [5] in remote forests. The integration is seamless, and the network of IoT sensors, gateways, and infrastructure is important for forestry conservation.

2. Framework in Theory

This research considers various theoretical aspects including the existing frameworks and concepts of the IoT and aligns with the

principles of deforestation. This study includes sensors and actuators and their integration for collecting and exchange of data for a quick decision-making process.

2.1. Key theoretical constructs

2.1.1. IoT ecosystem dynamics

The research in this direction leverages the concepts of the IoT and the framework being used for safeguarding forests.

2.1.2. Sustainable environmental practices

Various research frameworks on sustainable environmental practice use sensors of the IoT for conserving forest infrastructure.

2.1.3. Environmental protection via community centric

The opportunity of forest management helps in deriving a framework for environmental protection.

2.1.4. Guiding principles

The socio-ecological systems framework helps in founding the principles of IoT implementation with a critical foundation for the futuristic discussions of the IoT architecture in forest protection.

3. Architecture of Internet of Things (IoT)

The IoT is an important concept that deals with disparate sensors and actuators that can connect trillions of sensors to exchange data. However, the absence of a standard process that is accepted universally and the lack of references of the IoT architectures present a huge challenge. Literature studies helps in designing a common architecture tailored to specific applications, however with a wide focus on enabling the latest technologies of the IoT and various protocols at different layers relevant to our study in the context of the Chipko movement and illegal tree cutting.

The foundational model of the IoT architecture comprises three layers: application, network, and perception. However, certain papers and projects further refine these layers into middleware-based, service-oriented architecture (SOA)-based, and a five-layered architecture to differentiate the diverse application scenarios for future demands.

3.1. Application layer

At the application layer, IoT solutions are designed to cater to various use cases that solve challenges and represent them in a human-readable format. These involve refining the functionality and purpose of the IoT system, including data collection, processing, and analysis to represent the user in a meaningful way to take decisions via applications. In our case study, the primary focus is on developing a robust and efficient system for real-time tree surveillance, incident response, and prevention of illegal tree cutting. This layer's architecture must be tailored to enable seamless integration with actuators and sensor devices, data storage points, analytics, and decision-making components that are being integrated with each other to form an application layer.

3.2. Network layer

The network layer is responsible for ensuring seamless network communication and data transfer between the IoT sensors and actuators, sensor gateways, and the underlying architecture. The research evaluates various networking techniques such as Wi-Fi, Zigbee, LoRaWAN, and 5G, to play crucial roles in enabling reliable and low-latency communication methods. Given the

Figure 2
Illegal cutting of trees

remote and challenging locations where illegal tree cutting often occurs, the proposed network layer's architecture should be designed to address the least connectivity issues, thereby ensuring that the integrated data is secured over long and wide ranges.

3.3. Perception layer

The perception layer is one of the foundations of the IoT ecosystem that comprises sensors and actuators that are responsible for collecting various data from the physical environment [15] and trigger actions based on information received from sensors/actuators. In this context, the proposed perception layer will involve deploying various sensors or actuator nodes in the forest to monitor tree health conditions [16], its presence, and any of the suspicious activities related to illegal logging and cutting of the trees. The architecture must be optimized in ensuring an accurate and near timely data acquisition while conserving the least possible energy [3] to prolong the sensors and actuator nodes' operational life [16] span.

3.4. Middleware-based architecture

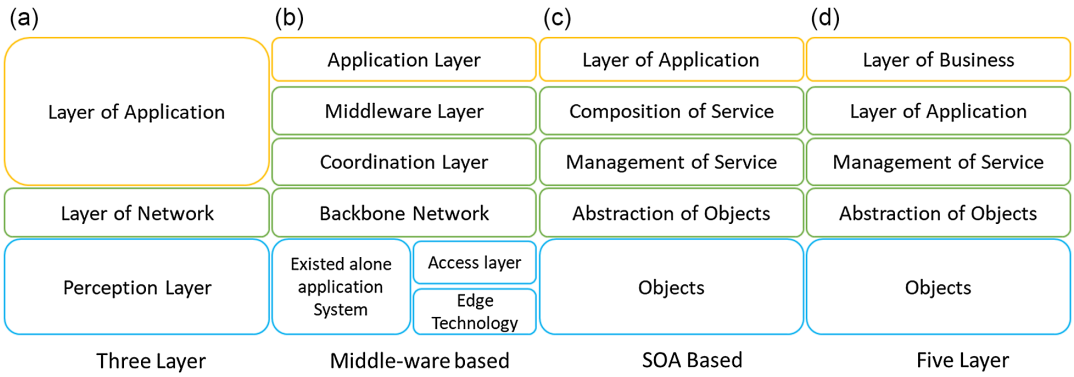
Data visualization, discovery, management, and security are the basic pillars of this middleware-based architecture.

3.5. Service-oriented architecture (SOA)-based

SOA-based architecture helps in real-time monitoring, incident response, and huge data analysis needed to work with IoT devices seamlessly.

Figure 3
Deforestation

Figure 4
IoT architecture



3.6. Five-layered architecture

The five-layered architecture utilizes components like data processing and logic. This architecture offers a framework for data management, analytics, and quick decision-making, enabling progressive data-driven analytics.

The challenges faced in the chipko movement and the illegal tree cutting process has been analysed to design a layered architecture. By understanding these architectures with the objectives, we will delve into the insights of the paper's organization.

The image in Figure 4 depicts the IoT architecture with various layered approaches.

4. Internet of Things (IoT) Architecture: A Comprehensive Overview

4.1. Layer of objects/perception layer

The perception layer is the foundation of the IoT as it lies in the layer of objects, also known as the perception layer. This layer comprises physical sensors and actuators that are important and responsible for collecting and processing diverse data. From temperature and humidity to motion actuation, vibration, and beyond, these sensors provide very important information about the environment [17]. Ensuring compatibility and seamless integration of heterogeneous objects, this perception layer employs standardized plug-and-play mechanisms [17]. Through secure orchestration channels, the perception layer digitizes and transfers data to the object abstraction layer [7, 17].

4.2. Object abstraction layer

This layer is also called as data transfer layer, which facilitates huge data transfer using radio frequency identification (RFID), global system for mobile communications (GSM), 3G, universal mobile telecommunication system (UMTS), Wi-Fi, Bluetooth Low Energy, and ZigBee.

This layer plays an important role in computing data and managing the data, ensuring the effectiveness and efficiency of operations in the ecosystem.

4.3. Service management layer

This layer, also called the layer of service management layer, also known as the middleware layer, is used for pairing sensors using addresses and names. This layer is used to abstract the data flow to make meaningful decisions. This layer utilizes network protocols for the management of services in the middleware.

4.4. Application layers

At the application layer, IoT systems provide valuable information to end users. For example, customers can ask for temperature and humidity measurements, indicating the significance of this layer in delivering high-quality smart [13] services. This layer serves as the interface for users to interact with sensors and access data from actuators. Also, this forms a business layer to produce advanced research insights and reports. Control mechanisms for data access are also a critical purview of this layer for computational requirements.

4.5. The business layer

The business layer, also called the management layer [17], helps in the overall orchestration of services of the IoT ecosystem. Gathering the data received from this layer develops models for business, graphs, and charts, pivotal to conduct advanced analysis [17]. This layer is also responsible for the design, implementation, evaluation, and monitoring of the IoT ecosystem. Decision-making has been supported by this layer that manages and monitors the four layers [10, 18–20]. By analyzing and comparing the results of the underlying layers to expected results, this layer orchestrates the continuous improvement of services [8, 13, 21]. Figure 5 represents RFID chip being punched on the trees.

5. Choosing the Right IoT Architecture

Though we have studied different IoT architecture and their models, all of them are not suitable for a real-world scenario of an IoT ecosystem. Three-layer architectures may not be useful for diverse technologies to transfer data between IoT platforms as their applicability is limited in nature. Also, SOA architectures such as a five-layer model exhibit few advantages such as communication between devices and integration of essential services while efficiently running on resource-constrained devices. This comprehensive yet straightforward architecture proves to be the most effective and practical model for IoT applications, offering a seamless user interface and robust computational capabilities.

By understanding the advantages of the five-layer architecture, we can design a secure architecture solution [2, 8] for deforestation using IoT.

Figure 5
Represent RFID (a chip being punched on the tree)

6. Empowering IoT: Unleashing the Building Blocks

To utilize the technology and its strengths of the IoT, the following six steps are crucial.

6.1. Identify

An important requirement to achieve our mission is to swiftly locate illegally felled trees due to any suspicious activities. Identification is one of our core IoT components, enabling naming and matching processes. Leveraging the cutting-edge technology such as electronic product codes (EPC) and ubiquitous codes (uCode), we will ensure seamless and unique identification of sensors cum objects and their respective addresses within the network communication channels [8]. IPv6, IPv4, and 6LoWPAN are being very instrumental in addressing IoT sensors and actuators.

6.2. Sense

Detecting unauthorized tree-cutting activities/methods is paramount, and the sensing methodology plays an important role for achieving this task. We will deploy smart sensors, actuators, and wearable sensing devices for these purposes to collect crucial data from networked objects [8]. This data cum information is further analyzed for triggering critical actions. Single-board computers were equipped with sensors, and built-in TCP/IP, with secure network protocols, serves as the critical foundation for IoT infrastructure to enable seamless network connectivity and critical data flow to a centralized user management portal for forestry department visualization purposes.

6.3. Communicate

There is a need to respond to the damage of the trees, and these must be responded to in near real time, making effective communication paramount. Seamless communication technologies in the IoT connect various sensors and actuator objects, facilitating the delivery of smart sensors. Being operated at a low power in the presence of noisy and lossy communication links, IoT sensor nodes use network protocols such as Wi-Fi, Bluetooth, IEEE 802.15.4, Z-wave, and LTE-Advanced. Near-field communication and RFID will enhance these capabilities. RFID in both modes, such as active, passive, or semi-active/active tags, emerges as one of our chosen communication methods due to its myriad advantages.

6.4. Compute

To communicate the critical incidents, we use microcontrollers and microprocessors. These act as the brains of the ecosystem and will exhibit high computational efficiency. Real-time operating systems (RTOS), such as TinyOS or Contiki, form the backbone of software platforms in our endeavor. Opting for TinyOS, with its minimal memory footprint and support for event-based programming, ensures a streamlined and efficient computation environment.

6.5. Services

Our IoT system built with a suite of services embraces four key categories: identity-related services, information aggregation services, collaborative-aware services, and ubiquitous services. Identity-related services are the foundation for ensuring the seamless virtual-to-real-world object transition. Information aggregation services gather and summarize raw sensory measurements for processing by IoT applications. Collaborative-aware services make informed decisions and take appropriate actions. Finally, ubiquitous services aim to provide seamless access to collaborative-aware services anytime and anywhere, catering to diverse forestry needs.

6.6. Semantic

Web technologies like Resource Description Framework and Web Ontology Language enable modeling, identification, and evaluation, leading to optimal judgments and delivery of services.

Table 1 summarizes the proposed samples and elements of our IoT.

Table 1
Elements of IoT and proposed samples

Elements of IoT	Proposed sample
Identification of naming and addressing of trees	Via uCode and IPv6
Sensing of trees	Via RFID tags
Communication	RFID, broker, gateways (rest to HTTP)
Computation	Smartphones with TinyOS software
Service	Ubiquitous
Semantic	OWL

7. Layer-Wise Architectural Protocols of IoT

7.1. Infrastructure (or) physical layer

The physical layer plays an important role in sensor/actuator communications. The EPC and unique identification number stored on RFID tags facilitate the identification of trees. RFID and their tags and reader help our architecture to seamlessly cater to IoT requirements (object IDs), making a secure architecture [8].

The RFID involves the radio signal transponder (tag) and the tag reader. RFID tags hold a chip that stores sensor identity, coupled with

Figure 6
RFID system architecture

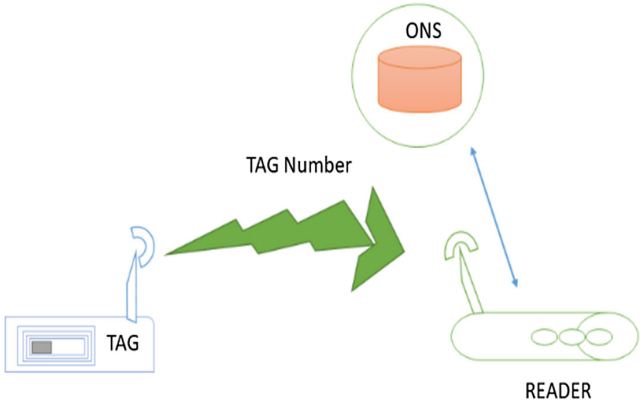
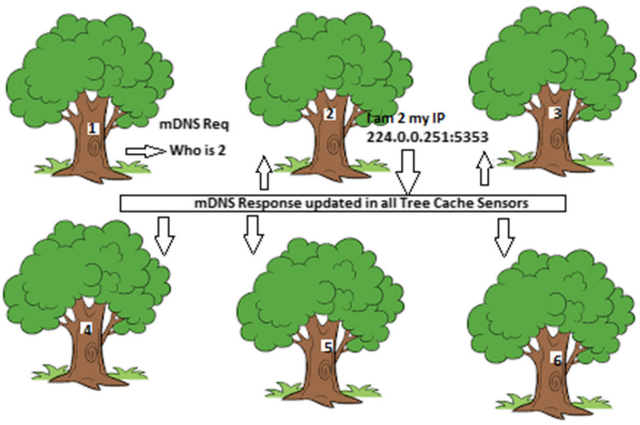


Figure 7
RFID service discovery



an antenna for radio wave communication with the tag reader. Utilizing radio frequency (RF) fields, the tag reader generates an RF to identify objects by reflecting radio waves from the RFID tag. As shown in Figure 6, this process involves transmitting the tag's number to the tag reader via radio waves, with subsequent relay to Object-Naming Services (ONS). The ONS searches the tag's details and interacts via a heartbeat with the broker, ensuring efficient data flow and communication.

In our experiment and research, we securely stamp RFID tags to trees in the forest, and tags allow discreet stamping at various locations on the trees.

Refer to Figure 6 for RFID system architecture.

7.1.1. Service discovery/networking protocol

Multicast DNS (mDNS) is being used as a choice for service discovery [1, 9, 14, 22].

mDNS will offer its flexibility to utilize the DNS namespace locally without additional configuration challenges, thereby eliminating the need for manual reconfiguration. This helps in operating without infrastructure, ensuring continuous functionality even during infrastructure failures. mDNS employs IP multicast messages to query names, attempting the nodes to multicast response messages containing their respective IP addresses. These responses update local caches on all network device sensors and actuators with the corresponding name and IP address, ensuring seamless service discovery (refer to Figure 7).

7.2. Layer of application

As the RFID receiver receives signals, the data will be transmitted seamlessly and passed to the application layer. The following application protocols are analyzed to fulfill this purpose effectively.

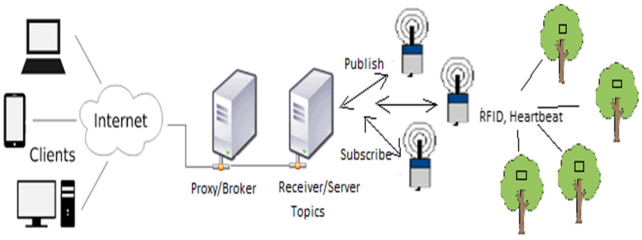
7.2.1. Constrained application protocol (CoAP)

CoAP, a widely used protocol by the internet engineering task force (IETF) Constrained RESTful Environments (CoRE) working group, stands as a vital application layer protocol for IoT applications. Built on HTTP, this protocol is based on the REST (Representational State Transfer) principles, CoAP offers a simpler way for clients and servers to exchange data over HTTP. The uniqueness of stateless client-server architecture enables clients and servers to expose and consume web services via Uniform Resource Identifiers. CoAP's default binding to UDP makes it more suitable for our IoT-based forestry preservation project, especially over low power consumption and lossy links. CoAP messages are categorized into confirmable, non-confirmable, reset, and acknowledgment. Like HTTP, CoAP supports methods such as GET, PUT, POST, and DELETE, enabling Create, Retrieve, Update, and Delete (CRUD) operations.

7.2.2. Message queue telemetry transport (MQTT)

MQTT, a message queue telemetry transport protocol developed for OASIS-standard messaging by Andy Stanford-Clark and Arlen Nipper, serves as an ideal connection protocol for our IoT forestry preservation project. Having the publish/subscribe pattern, MQTT ensures transition flexibility, connecting IoT devices, networks, and applications. It is well-suited for sensors and actuators that have limited resources, relying on unreliable or low bandwidth links. MQTT operates on the TCP protocol, offering three levels of QoS (quality of service) for message delivery. The subscriber, publisher, and broker in MQTT allow sensors or actuators to subscribe to specific topics and receive topic data from publishers via the broker as shown in Figure 8.

Figure 8
IoT architecture for forests



8. Top 6 Attack Vectors on the Proposed Solution

As we explore the top 12 security challenges [7, 23] in the IoT across various layers, we will reiterate the top 6 challenges in the IoT infrastructure.

First, the components often remain unnoticed, making them susceptible to physical attacks. Second, communication makes eavesdropping relatively easy. Lastly, the limited energy [15, 18]

and computing resources of many IoT components make it challenging to implement complex security measures.

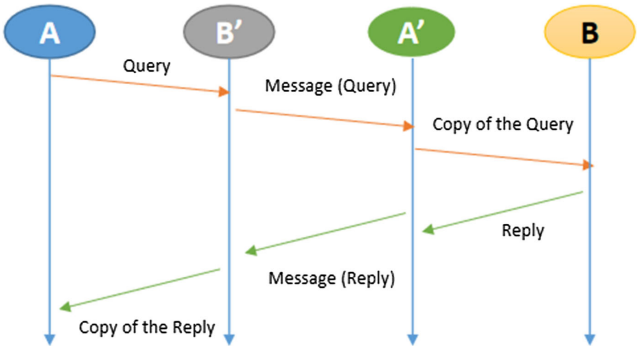
8.1. Threat vector 1: Data storage

Protecting the data securely in the database or in the data lakes becomes a critical threat to the infrastructure. To address this, Codo, a file system-level security solution for Contiki OS, offers secure data storage with improved performance through caching data for bulk encryption and decryption [22].

8.2. Threat vector 2: MITM (man in the middle)

RFID systems suffer from significant security flaws such as proxy attacks (MITM) [22]. The existing solutions fail to mitigate man-in-the-middle threats effectively (refer to Figure 9).

Figure 9
Manipulation/MITM of RF



8.3. Threat vector 3: RF-based identity theft

Steal the identity of node B by convincing node A to authenticate the attacker's transceiver B' as B, and vice versa. This attack relies on manipulating the RF signals between the nodes. Bypass encryption and authentication mechanisms are significant concerns for IoT for RF [22].

8.4. Threat vector 4: Encryption and authentication

Attacks on data for non-usage of encryption and authentication protocols such as TLS and DTLS and protocols like CoAP, MQTT, XMPP, and AMQP are being suffered from attacks.

8.5. Threat vector 5: Malware or virus via rogue sensors

The risk of malicious content delivered to IoT through payloads to underlying servers. These threats highlight the need for identifying and filtering out such malicious content to minimize damage to the entire infrastructure. There were challenges [7, 23, 24] related to access controls, software updates, trust, vendor security, intrusion detection, user and device access controls, privilege escalation, and logging concerns.

8.6. Threat vector 6: Unsecured communication

The possibility of MITM (man-in-the-middle) attacks due to unsecured communication channels in IoT systems. internal protocol securtiy (IPSec) acts as a mandatory security protocol for IPv6 network layer communication, which can help address this concern [5].

9. Secure Architecture Engineering Solution for Internet of Things (IoT)

As we study threat vectors in the previous session, the author proposes a secure architecture engineering [8, 9, 22] solution that aims to address these top 6 attack vectors and assist the emergency response team in safeguarding trees from deforestation.

To tackle issues such as RFID tampering (e.g., man-in-the-middle attacks), communication challenges, proxy tampering, denial of service attacks, and web application attacks related to deforestation, the secure architecture solution incorporates the following controls.

9.1. Secure architecture control-1

Implementing client and user whitelisting, IP address filtering, and protection against the top 10 Layer 7 attack vectors can resolve the mentioned issues effectively.

9.2. Secure architecture control-2

In designing the IoT architecture, it is essential to use trusted keys for heartbeats and sensor-secret keys for RFID sensors to authenticate themselves during installation.

9.3. Secure architecture control-3

For coding in the RTOS, a secure memory location must be chosen to prevent tampering. The software built on hardware should address known vulnerabilities, and the operating system should have the ability to revert to its original state even after being compromised.

9.4. Secure architecture control-4

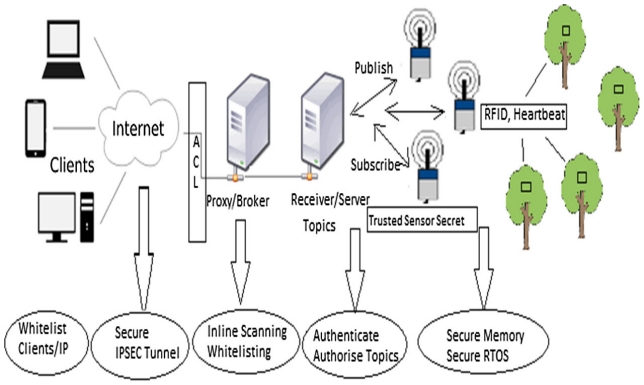
Using the topic published via message queue, publishers and consumers must ensure that data is not altered by either party. Whitelisting, authentication, and authorization play an important role in the architecture. Secure architecture principles need to be considered while designing Kafka topics or message queues.

9.5. Secure architecture control-5

Scanners need to be installed into the ecosystem to examine malicious systems such as virus and malware and must be inspected in-line. Transferring data shall only be allowed to whitelisted parties, and content scanning must be considered at the design level. Secure communication, especially via an IPSec tunnel, is suggested for content transfer using CoAP over MQTT to ensure the integrity of the data at rest and transit.

The proposed secure architecture and engineering solution for IoT (refer to Figure 10) helps in secure deforestation while mitigating the attack vectors and vulnerabilities [8].

Figure 10
Secure architecture engineering for forests using IoT



10. Conclusion

This paper addresses the theoretical gaps and practical implementation of the IoT in the ecosystem of the forests to help illegal mining of forestry. Using this research, we have addressed the top 6 threat vectors, historical challenges, and the secure architectural solution to mitigate these challenges effectively and efficiently. This research also proposed ways to solve the Chipko movement initiative using ever-evolving technology such as the IoT way.

11. Challenges and Future Directions

In the reality of IoT and forestry conservation, our study [17] acknowledges the persistent challenges of deforestation. While the secure architectural challenges presented in this paper as well as the articulations from the traditional things persist [16], future research endeavors should prioritize these aspects while exploring innovative applications of the IoT in forest digitalization [22].

12. Closing Remarks

As we conclude, with the technological innovation of the IoT, our research stands as a pillar for the progress of deforestation using the latest trend of IoT technology. As the globe navigates, we need to forge the technology ahead and present a sustainable future where our forests thrive and our planet flourishes [5, 12, 15].

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data available on request from the corresponding author upon reasonable request.

Author Contribution Statement

Sriranga Narasimha Gandhi Aryavalli: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Data curation, Writing – original draft, Writing – review & editing, Visualization, Project administration; **G. Hemantha Kumar:** Conceptualization, Methodology, Validation, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration.

References

[1] Martinez, E. C. (2021). IoT-driven solutions for water resource management. *WaterTech Quarterly*, *30*(2), 88–103.
[2] Smith, J. (2020). The Chipko movement: A historical perspective. *Environmental Conservation*, *45*(2), 123–136.
[3] Johnson, A. B., & Williams, C. D. (2019). IoT applications in environmental conservation: A comprehensive review. *Journal of Sustainable Technology*, *8*(3), 45–58.
[4] Green, M. (2017). The future of environmental preservation: IoT and beyond. *EcoTech Magazine*, *15*(4), 78–92.
[5] Sheng, Z., Yang, S., Yu, Y., Vasilakos, A. V., McCann, J. A., & Leung, K. K. (2013). A survey on the IETF protocol suite for the internet of things: Standards, challenges, and opportunities. *IEEE Wireless Communications*, *20*(6), 91–98.
[6] Chandra, R., Agarwal, S., & Singh, N. (2022). Semantic sensor network ontology based decision support system for forest fire management. *Ecological Informatics*, *72*, 101821. https://doi.org/10.1016/j.ecoinf.2022.101821
[7] Yang, D., Liu, F., & Liang, Y. (2010). A survey of the internet of things. In *Proceedings of the 1st International Conference on E-Business Intelligence*, 358–366.
[8] Aryavalli, S. N. G., & Kumar, H. (2023). Top 12 layer-wise security challenges and a secure architectural solution for Internet of Things. *Computers and Electrical Engineering, 105*, 108487. https://doi.org/10.1016/j.compeleceng.2022.108487
[9] Aryavalli, S. N. G., & Kumar, H. (2023). Layer-wise security challenges and a secure architectural solution for Internet of Things at physical, network and application layers. *Global Journal of Research in Engineering*.
[10] White, L. R. (2020). Enhancing biodiversity conservation through IoT innovations. *Conservation Science*, *18*(1), 22–38.
[11] Smith, A. (2018). Harnessing IoT for sustainable agriculture. *AgriTech Journal*, *10*(2), 45–60.
[12] Jackson, P. H. (2017). Connecting the dots: IoT's role in combatting climate change. *ClimateTech Insights*, *5*(1), 30–45.
[13] Parker, G. A. (2018). From smart homes to smart cities: Scaling up IoT for environmental impact. *Smart Systems Journal*, *22*(4), 180.
[14] Anderson, B. J. (2018). Empowering communities through IoT-based environmental monitoring. *Community Development Perspectives*, *12*(3), 75–90.
[15] Turner, R. W. (2019). Sustainable urban planning: A future with IoT integration. *Sustainable Cities and Society*, *40*, 210–225.
[16] Harris, L. M. (2022). Ecosystem health monitoring with IoT: Challenges and opportunities. *Environmental Monitoring and Assessment*, *50*(6), 275–290.
[17] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660.
[18] Johnson, S. P. (2019). Urban resilience and the Internet of Things: A comprehensive analysis. *Urban Studies Review*, *25*(3), 112–128.
[19] Adams, K. (2016). Beyond borders: Global applications of IoT in wildlife protection. *International Journal of Wildlife Studies*, *8*(4), 150–167.

[20] Rinkesh. (n.d.). *Deforestation – Causes, effects and solutions to clearing of forests.* Retrieved from: https://www.conserve-energy-future.com/causes-effects-solutions-of-deforestation.php

[21] Aryavalli, S. N. G., & Kumar, G. H. (2023). Safeguarding tomorrow: Strengthening IoT-enhanced immersive research spaces with state-of-the-art cybersecurity. *Archives of Advanced Engineering Science*, 1–9. https://doi.org/10.47852/bonviewAAES32021537

[22] Brown, E. R. (2018). Secure architecture engineering for IoT: Challenges and innovations. In *International Conference on Internet of Things Security*, 211–225.

[23] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges. In *10th International Conference on Frontiers of Information Technology*, 257–260.

[24] López, P., Fernández, D., Jara, A. J., & Skarmeta, A. F. (2013). Survey of Internet of Things technologies for clinical environments. In *International Conference on Advanced Information Networking and Applications Workshops*, 1349–1354. https://doi.org/10.1109/WAINA.2013.255

How to Cite: Aryavalli, S. N. G., & Kumar, G. H. (2024). Futuristic Vigilance: Empowering Chipko Movement with Cyber-Savvy IoT to Safeguard Forests. *Archives of Advanced Engineering Science*, *2*(4), 215–223. https://doi.org/10.47852/bonviewAAES32021480