IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, October 2026
Impact Factor: 8.2

A Survey on Verification of Security and Safety in IoT Systems

Prof. S. N. Avhad[1] and Ayush Kendhale[2]
Student, Information Technology[1]
Assistant Professor, Information Technology[2]
Adsul Technical Campus, Chas, India

Abstract: *The Internet of Things (IoT) connects devices such as sensors, smart home appliances, medical equipment, and industrial machines through the internet. These devices make many tasks easier and help different systems work efficiently. However, the growing number of connected devices also raises security and safety concerns; devices may face unauthorized access, data theft, cyberattacks, and unexpected failures. Security protects devices and information, while safety ensures devices operate properly without causing harm.*
This survey discusses the methods used to check the security and safety of IoT systems, the challenges involved, and possible ways to make these systems more reliable.

Keywords: Internet of Things

I. INTRODUCTION

The Internet of Things has become an important part of everyday life. It is used in smart homes, healthcare, agriculture, transportation, and industrial applications. IoT devices can collect data, share information, and perform tasks automatically, reducing the need for constant human involvement.
Despite these benefits, IoT technology also has certain risks. Devices connected to the internet may be exposed to cyberattacks, data leaks, and unauthorized access. In areas such as healthcare and industrial automation, these problems may create serious risks. Therefore, it is important to check whether an IoT system works correctly and protects the information it handles. Security and safety verification helps identify possible weaknesses and improve system reliability.

II. SYSTEM DESIGN

System Design

System design explains how the different parts of an IoT system are arranged and how they work together. In an IoT-based system, devices collect information from their surroundings, send it for processing, and provide the required output.

System Architecture

The proposed system can be divided into the following main components:

1. 1. Sensor Layer:

This layer includes sensors and connected devices that collect information from the surrounding environment. The collected data may include temperature, humidity, movement, and other measurements, depending on the application.

2. 2. Communication Layer:

This layer transfers data between IoT devices, gateways, and processing systems. Secure communication is important because it helps prevent unauthorized access, data interception, and information leakage.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, October 2026
Impact Factor: 8.2

3. 3. Processing Layer:

The processing layer handles the data received from IoT devices and sensors. It analyzes the collected information and performs the required operations based on the application. This layer helps the system understand the data and provide useful results.

Security and Verification Layer:

This layer checks whether devices and users are authorized to access the system. It may include authentication, encryption verification, software testing, and vulnerability assessment to identify possible security weaknesses.

Application Layer:

The application layer allows users to interact with the IoT system. This layer makes the IoT system easier to use and helps users respond to problems on time.

Working of the System

The Internet of Things has become an important part of everyday life. It is used in smart homes, healthcare, agriculture, transportation, and industrial applications. IoT devices collect data, share information, and perform tasks automatically, reducing the need for constant human involvement.

However, these systems may face security threats such as cyberattacks, data leaks, unauthorized access, and software errors. Therefore, it is necessary to verify whether an IoT system works correctly and operates safely.

During this process, security checks help protect data and prevent unauthorized access. If a problem is detected, the system may generate an alert or take appropriate action, depending on its design.

This allows users to check device status, view results, and identify potential problems. In this way, security and safety verification helps improve the reliability and proper functioning of IoT systems.

Security and Safety Considerations

Security and safety are essential when designing and using IoT systems. Devices should have proper security measures to ensure that only authorized users can access them.

Regular software updates and testing help identify errors and security weaknesses. It is also important to check how devices respond to failures and unusual situations.

III. EXISTING SYSTEM

Most existing IoT systems use security methods such as passwords, user authentication, encryption, and software testing to protect connected devices and the information they handle. Although these methods provide basic protection, some risks may remain.

For example, devices with weak passwords, outdated software, or insecure communication can become easy targets for attackers. Similarly, security measures that focus mainly on data protection may not identify problems caused by unexpected device behavior or technical failures.

Testing an IoT system for all possible errors and security threats can be challenging, particularly when many devices are connected.

These challenges highlight the need for verification methods that consider both security and safety. Regular testing, timely software updates, and continuous monitoring can help detect problems and improve the overall reliability of IoT systems.

IV. PROPOSED SYSTEM

The proposed system aims to improve the security and safe operation of IoT devices.

Sensors first collect information from the surroundings and send it to a processing unit through a network. Safety testing checks how devices respond to failures and unexpected situations.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 6, October 2026 Impact Factor: 8.2

If a problem is detected, the system can generate an alert so that the user can take appropriate action. Regular monitoring and software updates also help keep devices secure and reduce the risk of future problems.

The main objective of the proposed system is to check security and safety together. This approach can be used in healthcare, smart homes, agriculture, and industrial automation. Its effectiveness must be tested to determine how well it identifies problems and improves system reliability.

Advantages of the Proposed System

- Helps detect security weaknesses and software errors.
- Reduces the risk of unauthorized access to IoT devices.
- Checks how devices respond to failures and unexpected conditions.
- Supports regular monitoring and timely software updates.
- Addresses both security and safety during system verification.
- Can be adapted for different IoT applications based on their requirements.

V. EXPERIMENTAL SETUP

It helps check whether connected devices perform their tasks correctly, protect information, and respond appropriately to unexpected situations.

Hardware Requirements

The hardware required for testing may include IoT devices, sensors, a computer or laptop, and a network router. The exact hardware requirements depend on the type of IoT application being tested.

Software Requirements

The software setup may include an operating system, IoT development tools, monitoring applications, and security testing tools. These tools help verify that IoT devices communicate correctly, work as expected, and are protected against possible security threats.

Experimental Procedure

The testing process can be carried out in the following steps:

1. Device Setup: Connect the IoT devices and sensors to the network and configure them properly.
2. Data Collection: Collect sample data and check whether the devices send and receive information correctly.
3. Security Testing: Check authentication, access permissions, and data protection.
4. Software Testing: Examine the system for programming errors and unexpected device behavior.
5. Safety Testing: Check how devices respond to failures, unusual inputs, or potentially unsafe conditions.
6. Result Analysis: Record the observations and identify areas that may need improvement.

Evaluation Parameters

The system may be evaluated using parameters such as the number of security weaknesses identified, authentication performance, data protection, response time, and how well devices handle failures. These parameters can help assess the selected verification methods.

The experimental setup helps test the security and safety of IoT systems in an organized manner. The results should be clearly presented after testing the devices or running a simulation and recording the observations.

VI. RESULTS AND DISCUSSION

Suitable testing methods can reveal security weaknesses, software errors, and other problems that may affect the normal operation of connected devices.

Results

The expected outcomes of the proposed verification approach include the following:

- Improved Security: Authentication and access control can help restrict access to authorized users.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 6, October 2026 Impact Factor: 8.2

• Better Data Protection: Encryption can help protect sensitive information while it is stored or transferred between devices.
• - Early Detection of Errors: Software testing helps identify coding mistakes and unusual device behavior at an early stage.
• Detection of Security Weaknesses: Vulnerability assessment can identify areas that may require additional protection.
• Improved Safety: Safety testing can check whether devices respond properly to failures and unusual conditions.
• - Improved Reliability: Regular monitoring and testing help ensure that IoT devices continue to work properly.

Discussion

Different verification methods address different types of problems. Authentication controls who can access a device, while encryption helps protect information. Software testing and vulnerability assessment help identify errors and weaknesses, and safety testing examines how devices respond to unusual conditions.

Using these methods together can provide a more complete way to examine IoT systems. For example, devices with limited processing power may need lightweight security methods.

Regular monitoring and software updates are also important because new security weaknesses may appear over time. In applications such as healthcare and industrial automation, verification is particularly important because device failures may have serious consequences.

VII. LIMITATIONS AND PRACTICAL CONSTRAINTS

Each device has different features and capabilities, so the testing process and the problems identified may vary from one device to another.

1. Limited Device Resources: Many IoT devices have limited memory, processing power, and battery life. Because of these limitations, some advanced security methods may be difficult to implement without affecting device performance.
2. 1. Different Communication Standards: IoT devices use different communication protocols, making it difficult to use the same testing method for every device.
3. Increasing Security Threats: Devices may therefore require regular updates and additional protection to address changing threats.
4. Testing Complexity: Testing every possible error, attack, and failure condition is difficult, especially when many devices are connected to the same network.
5. Cost and Maintenance: Security tools, regular testing, and software updates require time, money, and technical knowledge.
6. Privacy Concerns: IoT devices may collect personal or sensitive information. Protecting this data during collection, storage, and communication is an important challenge.
7. Dependence on Network Connectivity: Some IoT systems depend on a stable internet connection.

These challenges show that one testing method may not work for every IoT system. Regular testing, updates, and monitoring can help address these issues and keep the system working reliably.

VIII. CONCLUSION AND FUTURE WORK

CONCLUSION

The Internet of Things has become an important technology in healthcare, smart homes, agriculture, transportation, and industrial automation. It allows devices to communicate, exchange information, and perform tasks automatically. However, the growing use of connected devices also raises concerns about security, privacy, and safety.

This survey explains various techniques used to check IoT system security and safety, including authentication, encryption, software testing, formal verification, vulnerability checks, and safety testing. Each method helps identify different types of problems and supports the proper functioning of connected devices. The discussion also covered

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, October 2026
Impact Factor: 8.2

challenges such as limited device resources, different communication standards, increasing security threats, and the difficulty of testing large IoT networks.

Security and safety should be checked at every stage of an IoT system, from its development to its daily use. Regular software updates, testing, and monitoring can help find problems early and improve system reliability.

Future Work

Future research can focus on developing verification methods that use fewer device resources while still providing suitable protection. Automated testing tools can also help developers identify software errors, security weaknesses, and other problems more efficiently. These tools can reduce manual effort and improve the reliability of IoT systems.

Future research can focus on combining security verification and safety analysis to identify both cyber threats and device-related problems. Studying these problems together can help developers detect risks early and make IoT systems safer and more reliable. Strong authentication, data privacy, secure communication, and regular software updates can further protect IoT devices from cyberattacks and other security threats.

These methods should be evaluated through practical experiments or computer simulations to understand how well they perform in real situations. This will help researchers understand the strengths and limitations of different approaches and select suitable methods for various IoT applications, such as smart homes, healthcare, industrial automation, and transportation.

REFERENCES

1) L.Abuserrieh and M. H. Alalfi, “A Survey on Verification of Security and Safety in IoT Systems,” IEEE Access, vol. 12,

2) M. Abbasi, M. Plaza-Hernández, J. Prieto, and J. M. Corchado, “Security in the Internet of Things Application Layer:

3) Requirements, Threats, and Solutions,” IEEE Access, vol. 10, pp. 97197–97216, 2022, doi:

4) B. Nazzal and M. H. Alalfi, “An Automated Approach for Privacy Leakage Identification in IoT Apps,” IEEE Access, vol. 10,

5) S. A. Ebad, “Quantifying IoT Security Parameters: An Assessment Framework,” IEEE Access, vol. 11, pp. 101087–101097

6) A. Mosenia and N. K. Jha, “A Comprehensive Study of Security of Internet-of-Things,” IEEE Transactions on Emerging

7) K. Boeckl, M. Fagan, W. Fisher, N. Lefkovitz, K. Megas, E. Nadeau, B. Piccarreta, D. O’Rourke, and K. Scarfone, “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks,” National Institute of Standards and Technology (NIST), NISTIR 8228, 2019. [Online]. Available: https://doi.org/10.6028/NIST.IR.8228.