

Need of Security in IoT

IoT devices sensors, networks और cloud services से जुड़े होते हैं। यदि security कमजोर हो, तो attacker device, data और पूरे network को नुकसान पहुँचा सकता है।

1 Why Security?

Security unauthorized access, data चोरी, device hijacking और service disruption से बचाती है।

2 Data Protection

Sensor data में location, health, habits और business information हो सकती है। इसे सुरक्षित रखना आवश्यक है।

3 Device Safety

सुरक्षा कमजोर होने पर attacker camera, lock, thermostat या industrial machine को नियंत्रित कर सकता है।

4 Trust और Reliability

Secure IoT system users का विश्वास बनाए रखता है और services को लगातार उपलब्ध रखता है।

Quick Visual



याद रखें:

Secure Device + Safe
Network = Trusted IoT

"Security को बाद में नहीं, design के समय से ही शामिल करें।"

Privacy for IoT Enabled Devices

IoT enabled devices लगातार data collect और transmit करते हैं। Privacy का उद्देश्य user की personal information पर उसका control बनाए रखना है।

1 Personal Data

Smart watch, camera, speaker और home assistant location, voice, health तथा usage data collect कर सकते हैं।

2 Consent

Data collect करने से पहले user को स्पष्ट जानकारी और permission मिलनी चाहिए।

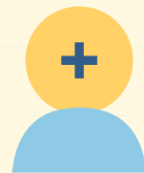
3 Data Minimization

केवल आवश्यक data ही collect करें और उसे उतने समय तक रखें जितना जरूरी हो।

4 Privacy Practices

Strong password, encryption, app permissions की जाँच और unnecessary microphone/camera access बंद रखें।

Quick Visual



याद रखें:

Secure Device + Safe
Network = Trusted IoT

"Security को बाद में नहीं, design के समय से ही शामिल करें।"

IoT Security for Consumer Devices

Consumer IoT devices जैसे smart TV, camera, router, bulb और speaker घर के network से जुड़े होते हैं। इनकी security user की daily privacy और safety के लिए महत्वपूर्ण है।

1 Default Password बदलें

Factory username और password को तुरंत बदलकर unique और strong password रखें।

2 Firmware Updates

Manufacturer के security patches और firmware updates नियमित रूप से install करें।

3 Secure Network

IoT devices को अलग Wi-Fi या guest network पर रखें और router का WPS अनावश्यक हो तो बंद करें।

4 Safe Usage

अनजान apps न install करें, unused services बंद करें और device बेचने से पहले factory reset करें।

Quick Visual



याद रखें:

Secure Device + Safe
Network = Trusted IoT

"Security को बाद में नहीं, design के समय से ही शामिल करें।"

Security Levels in IoT

IoT security को अलग-अलग levels पर लागू किया जाता है, ताकि device से cloud तक पूरे ecosystem की सुरक्षा हो सके।

1 Device Level

Secure boot, hardware protection, strong authentication और tamper detection device को सुरक्षित रखते हैं।

2 Network Level

Firewall, secure Wi-Fi, segmentation और TLS जैसी तकनीकें communication को protect करती हैं।

3 Application Level

Secure coding, access control, input validation और regular testing application attacks रोकते हैं।

4 Cloud और Data Level

Encryption, backup, audit logs और role-based access data तथा cloud services की रक्षा करते हैं।

Quick Visual



याद रखें:

Secure Device + Safe
Network = Trusted IoT

"Security को बाद में नहीं, design के समय से ही शामिल करें।"

Protecting IoT Devices

IoT device protection के लिए prevention, detection और response—तीनों की आवश्यकता होती है।
Security एक continuous process है।

1 Authentication

हर device और user की identity verify करें। Multi-factor authentication उपलब्ध हो तो उसे enable करें।

2 Encryption

Data को transmission और storage दोनों समय encrypt करें, ताकि चोरी होने पर भी वह पढ़ा न जा सके।

3 Monitoring

Unusual login, traffic या device behavior को monitor करें और alerts लगायें।

4 Incident Response

Attack होने पर device isolate करें, credentials बदलें, logs जाँचें और patched backup से restore करें।

Quick Visual



याद रखें:

Secure Device + Safe
Network = Trusted IoT

“Security को बाद में नहीं, design के समय से ही शामिल करें।”

Future IoT Ecosystem और Powerful Core

भविष्य का IoT ecosystem लाखों devices, edge computing, cloud और AI services से मिलकर बनेगा।
Secure algorithms के लिए powerful core और efficient processing आवश्यक होगी।

1 Powerful Core की आवश्यकता

Advanced encryption, real-time analytics और AI models को चलाने के लिए तेज CPU, secure hardware और पर्याप्त memory चाहिए।

2 Edge Computing

Data को cloud पर भेजने से पहले edge device पर process करने से latency कम और privacy बेहतर होती है।

3 Secure by Design

Security को product के अंत में जोड़ने के बजाय design, hardware, software और update system में शुरू से शामिल करें।

4 Sustainable IoT

Future devices कम power में अधिक काम करेंगे और energy-efficient security algorithms का उपयोग करेंगे।

Quick Visual



याद रखें:

Secure Device + Safe
Network = Trusted IoT

"Security को बाद में नहीं, design के समय से ही शामिल करें।"

New Trends: AI और ML का IoT में प्रवेश

AI और ML IoT devices को केवल data collect करने से आगे बढ़ाकर सीखने, अनुमान लगाने और अपने-आप निर्णय लेने में सक्षम बनाते हैं।

1 Predictive Maintenance

ML sensor data से machine failure का पहले अनुमान लगाकर timely maintenance में सहायता करता है।

2 Smart Detection

AI camera और sensors unusual movement, fraud, intrusion या abnormal behavior पहचान सकते हैं।

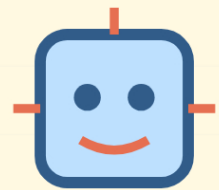
3 Automation

Smart home, healthcare, agriculture और industry में AI data के आधार पर automatic actions लेता है।

4 Security Challenges

AI models को गलत data, adversarial attacks और privacy risks से बचाना आवश्यक है; human oversight बनाए रखें।

Quick Visual



याद रखें:

Secure Device + Safe
Network = Trusted IoT

"Security को बाद में नहीं, design के समय से ही शामिल करें।"