IOT AND SMART SECURITY SYSTEMS: HOME AND URBAN SURVEILLANCE AND SAFETY

Shirinov G M
Tashkent State Technical University, Tashkent, Republic of Uzbekistan email: ganjimurod@gmail.com
Gulomov A A
Student of group 186-22 RQT in the "Radioelectronic Devices and Systems" program at Tashkent State Technical University email: alishergulomov25@gmail.com

Abstract: *This article analyzes the application of the Internet of Things (IoT) and related smart technologies in managing home and urban security, smart home systems, intelligent locks, enhanced video surveillance, and associated security measures. It examines IoT devices, Smart City initiatives, and the use of AI and ML algorithms to improve the efficiency of video surveillance systems, as well as the security challenges and recommendations for their mitigation. The findings highlight the current and future development prospects of IoT-based smart security systems and their significance in ensuring the safety of society and urban transport infrastructure.*

Keywords: *Internet of Things (IoT), smart home, video surveillance, enhanced functionality, Smart City, intelligent locks, AI and ML, security, cloud storage, network security.*

When we imagine the use of IoT technologies in modern security systems, the concept of a “Smart House” immediately comes to mind. Today, these technologies are widely applied not only in government institutions and large enterprises but also in residential and office buildings.

People are increasingly relying on IoT devices to protect their personal data, families, and property. Such devices allow users to receive real-time information, receive security alerts, and control home systems remotely, making daily life both safer and more convenient.

The year 2016 marked a turning point when IoT technologies began to have a significant impact on home security. According to Google Trends, global searches for the term “smart home” increased by more than 75% compared to 2015, reflecting the growing public interest and trust in smart technologies.

IoT-enabled systems made it possible for people to control door locks, lighting, heating, cameras, and even radios through their smartphones, giving them the ability to monitor and manage home safety from anywhere in the world.

One of the main drivers behind the increasing interest in smart homes is the development of IoT-based systems that are efficient, energy-saving, and user-friendly.

These innovations not only enhance security but also improve comfort and energy efficiency, transforming IoT into a global trend that improves the quality of life, strengthens safety, and simplifies human activity.

Smart home security has become an integral part of modern living, motivating many people to convert their residences into interconnected, intelligent environments. Surveys indicate that more than 90% of consumers cite security as a primary reason for purchasing smart home systems, which has driven significant market growth in security-related technologies. The popularization of smart locks in 2016 further accelerated this trend.

Contemporary smart locks provide alternatives to traditional keys by enabling digital authentication methods such as biometric recognition, PIN codes, and remote unlocking via smartphone apps. These systems automatically log when doors are locked or unlocked and send real-time notifications to users' mobile devices, substantially enhancing homeowners' ability to monitor and control access. Smart home security typically integrates multiple subsystems-cameras, motion sensors, smoke detectors, and lighting controls-to provide layered protection.

The integration of devices improves event detection and reduces false alarms; for example, combining motion sensors with video verification allows for more accurate identification of genuine threats.

However, these capabilities introduce new risks. Because IoT devices are connected to the internet, they can be vulnerable to cyberattacks; therefore, manufacturers and users must adopt strong security measures such as encryption, regular firmware updates, robust authentication, and network segmentation. Rigorous protocols are also required to protect personal data and manage user permissions responsibly.

In the future, the application of artificial intelligence and machine learning within smart home security will likely enhance threat prediction, enable context-aware responses, and automate resource management. Achieving reliable and resilient systems will require coordinated technical, legal, and ethical efforts to ensure both functionality and user trust.

Smart locks and alarm systems have revolutionized modern home security, becoming one of the defining achievements of IoT-based technology. In the summer of 2016, the second-generation Kevo smart locks were released, allowing users to control home access with greater precision and flexibility [1-2]. These locks not only provided digital keyless entry but also enabled homeowners to grant temporary access to others for specific time periods.

This feature proved highly practical for delivery services, maintenance personnel, and other short-term visitors who required limited access authorization. Among the most remarkable IoT advancements of that year was the Eelosk iris-based authentication system. Initially perceived as a futuristic concept, it soon became a tangible innovation.

Eelosk's technology identifies users through iris recognition, dramatically enhancing security by making unauthorized entry virtually impossible. The system has since been

adopted not only in smart homes but also in business centers, government facilities, and high-security infrastructures.

In January 2016, Eelosk expanded its platform by introducing new applications such as multi-factor authentication, access logging, and biometric data protection modules. What was once science fiction - unlocking doors with a simple eye scan - became a reality.

Fig.1. Mutual integration of IoT technologies in a Smart home

At the same time, established security companies began embracing IoT integration. The well-known Yale brand, recognized for its reliability in home protection, launched its first smart lock at the end of 2015 and followed up with a series of smart alarm systems in 2016. Through its Yale Assure application, users could operate locks using a digital key, QR scan, or Bluetooth connection, simplifying access control and strengthening overall home safety. Consequently, 2016 can be regarded as a pivotal year in the evolution of smart locks and alarms. These innovations laid the foundation for future IoT-driven ecosystems, integrating artificial intelligence and predictive analytics to create safer, smarter, and more adaptive home security solutions.

Among the leaders shaping the modern smart security landscape, ADT has played a pioneering role by launching its “ADT Smart Home” system, which allows users to manage and monitor home security remotely. This innovation not only enables homeowners to control locks, alarms, and sensors in real time from virtually anywhere, but also reflects the company’s commitment to providing advanced, technology-driven protection solutions.

The platform supports live monitoring, automatic alerts, and integration with other IoT devices, creating a cohesive and responsive home security ecosystem. Another revolutionary milestone in smart surveillance emerged in 2015 with the beta release of the Manything 4 application.

This software transformed unused smartphones and tablets into functional security cameras capable of live streaming, motion detection, and cloud-based recording. While the base version supported one free camera, premium subscriptions allowed multiple cameras and extended cloud storage [3]. The app’s compatibility with the IFTTT (If This

Then That) automation service enabled users to receive real-time email or text notifications when specific events occurred, enhancing situational awareness and responsiveness. In the same period, the iSmartAlarm team introduced the Spot smart camera — a compact yet powerful device designed to bring affordable and efficient monitoring to everyday households. Spot offered innovative features such as sound detection (alerting users when smoke or carbon monoxide alarms were triggered), time-lapse video creation, and 360-degree rotational adjustment. With its flexible mount, wall installation capability, and setup time of under three minutes, Spot quickly became a practical and accessible choice for home users. Together, these developments marked a transformative step in home surveillance, redefining the boundaries of convenience and protection. IoT-based cameras and monitoring systems now allow homeowners not only to observe but also to interact with and automate their environments. As a result, smart monitoring has evolved into a cornerstone of modern digital security, providing both peace of mind and intelligent situational control.

The period from 2020 to 2030 is recognized as the era of the Internet of Things (IoT). Currently, approximately 26 billion devices are connected to the internet, with a combined economic value of around 1.7 trillion dollars. This figure is nearly double the number of connected devices from five years ago and includes not only household and office equipment but also vehicles, industrial machinery, and everyday objects equipped with web connectivity. It is estimated that by the next few years, 98% of vehicles will be connected to the internet.

As IoT systems become more complex, technologies for correlating and analyzing data are also evolving. Companies are moving beyond real-time monitoring to leverage predictive analytics and proactive insights. This shift enables more efficient resource management and reduces operational risks. One of the key strategies for expanding IoT-based safety and operational efficiency is the implementation of Smart City projects. While several such initiatives have recently begun in the United States, internationally these programs have already advanced significantly. For instance, in 2017, the United Arab Emirates passed legislation requiring all targeted buildings to be connected to the Hassantuk security network of the Ministry of Interior. This program, under the “Smart and Safe City” concept, aims to centrally monitor fire and life safety events while reducing inspection costs for over 150,000 buildings across the UAE. Modernizing urban infrastructure through transport network upgrades represents an essential first step in the evolution of Smart Cities. Many transport operators now use large-scale public data to identify opportunities for infrastructure redesign and enhancement. Cities can employ sensors installed in public transport systems, railways, and roads to collect and analyze data at integrated security operation centers. Applications include monitoring traffic signals, ensuring pedestrian crossing safety, and optimizing the placement of STOP signs, among others. Leveraging IoT for security management not only enables rapid short-term responses but also improves long-term risk mitigation strategies. The integration of

artificial intelligence and predictive analytics facilitates the creation of more efficient, intelligent, and integrated urban transport and security ecosystems.

The Internet of Things (IoT) and related advanced technologies play a pivotal role in driving significant societal transformations today. These technologies enable users to interact with their environment, collect and analyze data in real time, and enhance decision-making processes. Moreover, IoT and smart systems improve functionality across various sectors, facilitating new services, optimized resource management strategies, and innovative security solutions. The field of video surveillance has experienced a profound evolution due to IoT technologies. Traditional cameras are increasingly being replaced by intelligent video surveillance systems that not only detect motion and provide live streaming but also incorporate facial recognition, predictive threat analysis, automated alerts, and cloud storage capabilities [4]. Consequently, IoT-based surveillance systems elevate safety standards while transforming the monitoring of cities, homes, and businesses into an efficient, smart, and interactive process.

Fig.2. External appearance of a modern security camera

When IoT-based smart monitors and sensors are combined with high-speed network solutions, the efficiency and functionality of video surveillance systems are significantly enhanced. This integration provides users with real-time monitoring, automated alerts, and advanced analytical capabilities, enabling intelligent management of urban, office, and residential infrastructures in addition to strengthening security.

- Artificial intelligence (AI) and advanced machine learning (ML) analytics are leading to unmanned video surveillance. Reliable programmed AI systems enable the deployment of extensive networks of surveillance equipment without human oversight.
- Wireless communication technologies such as 5G and Narrowband IoT (NB-IoT) improve the speed of video feed delivery for human and artificial intelligence applications.
- Reduced latency enhances the performance of video systems and expands user capabilities.
- The signal transmission capability of NB-IoT enables the placement of video cameras in locations that were previously inaccessible.

- Manufacturers will benefit in many ways from improved video surveillance. Worker safety can be enhanced by restricting access to hazardous areas. Automated assembly line monitoring can ensure the fulfillment of production goals and quickly address incidents. Smart systems connected to IoT-based video cameras enable predictive maintenance, which leads to more efficient operation of the factory.
- Smart homes equipped with IoT-enabled video surveillance systems can detect and restrict young children or pets from entering hazardous areas.
- Smart cities are implementing modern IoT video surveillance to monitor vehicle and pedestrian traffic and address congestion issues. Predictive artificial intelligence analysis can detect potentially dangerous situations before they escalate and provide decision-makers with sufficient time to respond. This information also helps prevent disasters such as recent catastrophic weather events.
- Physical security is enhanced by several modern security systems incorporating IoT-supported video surveillance. Smart drones can minimize challenges associated with monitoring large areas such as airports and train stations.
- Facial recognition software can be used to identify authorized personnel and restrict unauthorized individuals from entering secure facilities.

The adoption of IoT introduces complex security challenges that must be addressed to realize the full potential of advanced video surveillance.

Every smart camera represents an attack vector: improperly configured or outdated firmware can allow attackers to access video feeds, authentication credentials, and sensitive metadata (e.g., timestamps, geolocation, device identifiers).

Connected devices can also be repurposed as computational resources for malicious activities-such as botnets, cryptocurrency mining, or distributed denial-of-service (DDoS) attacks.

A compromise of an IoT camera frequently undermines the integrity of the entire system: attackers may move laterally within the network to reach other devices, central servers, or cloud services.

Supply-chain weaknesses and vulnerabilities in vendor infrastructure can enable tampering with or deletion of surveillance data. Therefore, cameras and their management platforms require stringent security controls-secure boot, signed firmware, encryption, strong authentication, and reliable update mechanisms.

Protecting personal data is another critical concern: unauthorized access to video footage and biometric identifiers can result in severe privacy violations and legal consequences. Mitigations such as network segmentation, least-privilege access controls, transport-layer security (TLS) or VPN tunnels, and certificate-based authentication substantially reduce compromise risk.

In summary, while IoT-connected video surveillance systems offer significant capabilities, securing them demands a holistic, multi-layered approach spanning device, network, cloud, and operational processes.

Robust architecture, continuous patching, active monitoring, and incident response procedures are essential-because a single weak point can jeopardize the entire infrastructure.

REFERENCES:

1. Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things-A survey of topics and trends. Information Systems Frontiers, 17(2), 261–274.

2. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164.

3. Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context aware computing for the Internet of Things: A survey. IEEE Communications Surveys & Tutorials, 16(1), 414–454.

4. Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. Journal of Cleaner Production, 140, 1454–1464.