International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

AI-DRIVEN PRIVACY AND SECURITY FRAMEWORKS FOR SMART HOMES: A COMPREHENSIVE SURVEY

Abhay Kumar Ray[1*], Dr. Rupak Sharma[2], Dr. Sunil Kumar Pandey[3]

[1]Research Scholar, Department of Computer Applications SRM- Institute of Science and Technology, Delhi –NCR Campus, Modinagar -201204, Ghaziabad, India

[2]Associate Professor, Department of Computer Applications, SRM- Institute of Science and Technology, Delhi –NCR Campus, Modinagar -201240, Ghaziabad, India

[3]Professor, Department of IT, Institute of Technology & Science, Mohan Nagar- 201007, Ghaziabad, India

[1]ar2587@srmist.edu.in; [2]rupaks@srmist.edu.in; [3]sunilpandey@its.edu.in

*Corresponding Author: ar2587@srmist.edu.in; https://orcid.org/0009-0005-6990-7238

Abstract

Smart homes have major evolution in residential automation, which integrates Internet of Things (IoT) technologies to improve comfort, energy efficiency, and remote accessibility. Widespread adoption of smart home systems has faced critical privacy and security challenges due to uses of heterogeneous communication protocols, constrained computational power of sensor nodes, and lack of standardized encryption authentication mechanisms and strong AI based attack detection and mitigation system. This paper presents a comprehensive survey of privacy and security issues in IoT-enabled smart homes, emphasizing on vulnerabilities at the different layers of IoT communication system. It discussed major communication protocols ZigBee, Bluetooth, Wi-Fi, Z-Wave, 6LoWPAN, LoRaWAN, and NFC and highlighting their operational weaknesses and potential attack vectors such as denial-of-service, spoofing, replay, and man-in-the-middle attacks. A systematic research methodology was applied to analyze 56 key publications from 2014 to 2025 drawn from IEEE, Scopus, Springer, arxiv journal and MDPI databases. The reviewed studies reveal a growing application of Artificial Intelligence (AI) and Machine Learning (ML) methods for intrusion detection, anomaly recognition, and adaptive security enhancement. Findings indicate a clear transition from traditional cryptographic protection toward intelligent, data-driven, and decentralized security frameworks. The study identifies major research gaps related to data integrity, edge level AI based attack detection system implementation, federated learning, and explainable AI for security and privacy improvement IOT ecosystem. ML techniques (DT, RF, ANN, CNN, and LSTM,) demonstrated over 90% accuracy in attack detection, yet issues such as protocol vulnerabilities, data privacy, and limited computation capabilities remain. The review highlights the need for lightweight, explainable, and privacy-preserving IDS solutions to strengthen security in resource-constrained smart home environments.

Keywords: Smart Homes, IoT, IoT security, Privacy, IoT communication protocols, AI & ML, Attack identification and Classification.

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1. Introduction

"Smart Home" is generally used to describe a residence that has set of smart appliances for entertainment, interactive consoles, cooling and heating system, lighting, locking system, smoke or fire safety system, IP enabled cameras etc. These smart devices are not only capable to communicate with one another but also sharing real time data and store the same locally or remotely and the entire home can be controlled locally or remotely from any location in the home or from any location by the use of smart phones or computers. In another words, a smart home provides sense of security and safety, energy efficiency, comfort and conveyance, easy to operate and access at real time to the owner at all time. The rapid changes in digital technologies in terms of services, architecture, and development in the internet have influenced the smart home technology which is creating its own significance in the today's market place. Revenue in the Smart Home market in India is expected to reach US$ 4.87 bn, US$31.5 bn in USA and US$26 bn in Europe by the end of year 2022. The revenue is predictable to show an annual expansion rate (CAGR 2022-2026) of 13.52%, consequential in an estimated market volume of US$8.08bn and the count of active households is projected to amount to 54.0m users by 2026 in India.[1].

Smart homes have some advance and properly developed systems beyond the elementary functionality like automatic door openers, smart lighting control system, safety and security system to offer many tangible advantages in terms energy efficiency better control and operation in terms of operational cost efficiency for long term. IP-enabled security cameras, security alert or notification system, object motion detection sensors based intrusion detection system, water uses related system, smart door locks etc. to provide better safety and security at home. Taking view of these kinds of needs of automations in the smart homes it need an innovative and interdisciplinary technologies, so that it can provides services anytime, flawless connection for data and real time status sharing among the devices or sensor nodes embedded in different home appliances is internet of Things (IOT).

The Internet of things (IoT) is basically use to refer an interconnection of physical devices which are not conventionally referred as electric items and these devices don't have computational and communications power like motor vehicle, water pumps, buildings, doors, parking areas, dustbins etc. These items can possess some microcontroller or microprocessor, controlling software, sets of sensors, actuators, and connectivity capability using some standard protocols, by which these devices can collect and exchange data and their status. Now as days, the IoT is capable enough to connect and provides computational power to large number of diverse and heterogeneous devices. IoT can also provide connection for man to device, device to cloud, device to device for open access and selective access of selected subsets of sensor data for the development and design of large scale of digital services [2]. To develop a generic architecture of IoT based smart homes is very complex and need high skill set, because of the extremely large range of home appliances and venders support, embedded technologies, communication protocols at different layer of network and information technology services that are involved in such systems.

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A. Basic connectivity architecture of smart homes [3]

The components required for Smart Homes are:

1. Set of diverse verity of sensors and actuators like PIR sensors, smoke sensors
2. Connectivity protocols supporting to IoT
3. Microprocessors or Microcontrollers chips to control and actuate the connected appliances.
4. Smart home local server or a central controller device to store and forward data to fog and cloud layer and also capable to accept command form the web by the smart home user
5. Web applications and Mobile application for remote access of services or devices. With help of above mentioned resources, the smart homes can implement successfully. The basic services and their communication model or the smart home network like in figure-1 as given below.

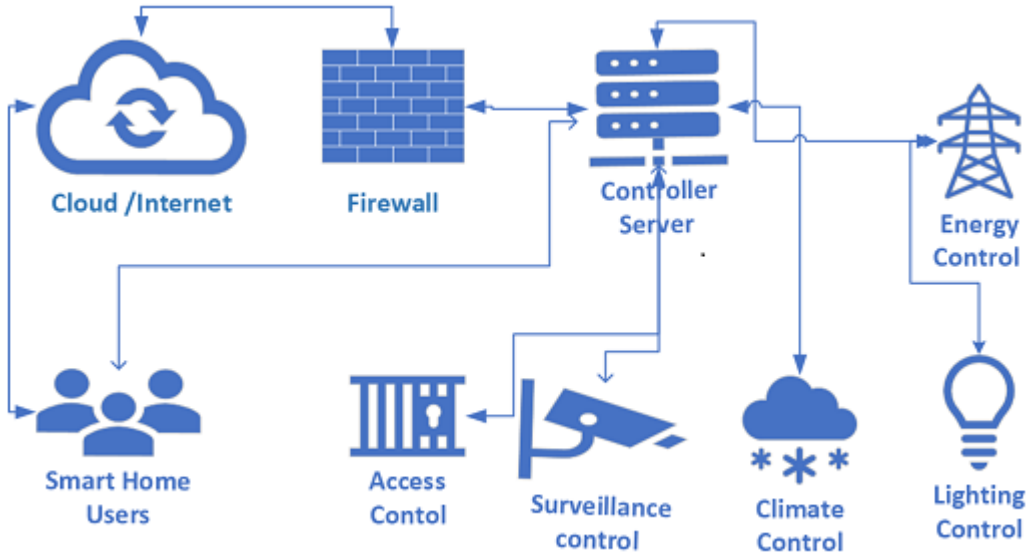


Figure 1: (Basic Modules and communication models of Smart home)

The Smart home controller server is central service provider in basic model of smart home and it is connected to the cloud or home owner via security firewall when the owner try to access its services using internet and owner can directly get connection locally via some application. It can be a general purpose computer and act like a gateway for outsider, and it has capability to store sensed data and having analytical processing capability with cloud support. Controller server can accept commands to activate or deactivate any services via internet or intranet by authorized users. This device also acts like a network address resolution and identification of device. Controller server has several of services like authorization and identification of legitimate user, device controlling or actuating capability via commands or signals, device Configuration management, analytical Services and device discovery services.

2. Security and privacy issues and challenges

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Today many buildings already have sensors for attempting to implement smart service like smart Water sprinkler, smart energy management services, Auto-curtain, automatic gates, IP enable smart camera, and in this way home automation is occurring. Smart home network security must have six essential attributes of privacy and security like Confidentiality, Integrity, Non-repudiation, Authorization & Authorization and Availability. Many security experts worry that IoT (nicknamed the "Internet of Threats" by Kaspersky Lab's founder) is going to make hacking exponentially more common once many people begin buying insecure smart devices for their homes. This is evolution of existing communication protocol must have security and privacy mechanism at every layer of communication. Every smart system must have built-in high level of security that's enabled by default and mandatory for all devices.

Therefore, every smart home appliance must be secure in context of unauthorized physical access, data access and configuration access. Smart homes have connected smart devices and have opened a security risk window or point of entry for intruder or hackers to our smart home can be spied and it will be a new opportunity for cybercriminals [4]. For simplicity consider some cases as given below.

- What if a hacker get accesses of data of a smart appliances including electricity uses (smart meter), status of entertainment devices or smart camera on the basis of uses trends hacker 1can figure out the owner or his/her family members are inside the home or out stationed. So it becomes very easy to commit crime.
- What if a black hat hacker gain access of the smart home network or smart lock system due any vulnerability or weak security policy for ransomware attack on smart home environment and make someone hostage. A huge ransom might be demanded to release someone or to restore the working of the smart system too.
- Smart home security issues must be categorized into technological challenges and security challenges. IoT devices are heterogeneous and ubiquitous in nature, which contributes to technical challenges mainly related to wireless communication technology, huge scalability, distributed nature, and energy efficiency. On the other hand, security challenges include authentication for process, applications, person and device, confidentiality of data in transit as well as in rest, data and device to device connection integrity, and end-to-end security.
- Smart home security must have confidentiality, integrity, and availability (CIA) which also applicable for its connected device and achieving these goals creates a challenge, considering in terms of computational power and resources available for smart home subsystems.

The security and privacy related issues may occur at different level of design, deployment and, implementation of smart home system [5].

a) Perception Layer (Sensor node Layer)
b) Communication Layer
c) Application Layer

a) Perception Layer: The primary objective of perception layer or sensor layer is sense the physical phenomenon or changes in installed environment and collects data with the help of different sensor and sends the data to the local controller device via any wired or wireless

Received: August 01, 2025

Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

communication technology. At this layer data sensing taken place and huge volume of data generally in hundreds of GB par day taken place [7]. The major security threats and security challenges at this layer is physical security (tempering of devices), Intercepting of communication medium , Limited power of computation so data confidentiality can compromised at some extent , lack of cryptographic approach, replay attacks.

b) **Communication Layer:** This layer is responsible for data routing and transmission of sensed data to different IoT hubs and computational devices connected to internet, intranet and extranet. The major security and privacy challenges are as given below.

- Data security and privacy is always on risk due to remote access and data exchanges among devices using wireless communication protocols.
- Every communication protocols [6](Thread , 6lowpan, Bluetooth, Wifi, Z-wave Zigbee , Sigfox, NFC, LoRa, COAP, XMPP,http, https) has their own security issues and vulnerabilities while using in smart home environment
- All the security issues and vulnerabilities that exist in wired network applicable to the wireless technologies too.
- Hackers may gain unauthorized access to smart home network or server through wireless connections, bypassing any firewall protections so we need much more security mechanism.
- Sensed data is generally not encrypted while transmission so it has risk of intercepted and disclosed.
- DoS , DDos ,or bot attacks may directed at wireless connections or devices.
- Malicious code or some virus may corrupt sensed data on the sensor node before transmitting and it can be happening in wired network connection too.
- Internal attacks or internal data leaks are always possible due to ad hoc transmissions.
- C) Application Layer: The application layer smart home based on IoT infrastructure provides an easy to use, easily maintainable, scalable, secure and smart environment. Application layer must provide the strong authenticity including context awareness, data integrity, privacy and confidentiality of the data. At this layer security challenges are as given below.
- It is very challenging to integrate verity of applications which has different authentication mechanisms including (Person, Process, devices and context) to ensure data privacy and accessibility and identity authentication and authentication
- Many smart devices like IP enable cameras, object tacking devices cause large overheads on applications and server for analyzing the data, impacting the availability of service. So the architecture of smart home must have support of service oriented approach and n-tier architecture which enable to provide essential features at peak time.
- Perception layer has limited amount of processing capability, so strong cryptographic approach included in this layer for data in rest or under the transmission from server to server communication or application to application communication.

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Third party application services or APIs may have some malicious entities to gain access the data of smart home to the dark web.
- Smart home must have proper AI enable tools to analyze and senses security leak intrusion in the application layer and control the amount of data to be disclosed safely, and how and which way it should use, and by whom.

3. Methodology for Research survey

The process of this study commences with the clear a comprehending smart home security and privacy maintenance with AI, which leads the study to identify fundamental threats and examine AI solutions for security, performance standards, and metrics. This directed our initial data collection and focusing scope of study to understand the problem. To understand the problem well, structured search strategies are employed on data collections. The data sets are scholarly collections that include IEEE, Scopus, Springer, and the ACM Digital Library. To increase accuracy, smart home, smart home security, AI in the IoT, machine learning for cyber threats, security and privacy preservation were the search terms. The inclusion and exclusion criteria were set to identify the relevant peer-reviewed publication from and between 2014 and 2024 and to excluding non-technical papers, antiquated literature, and irrelevant work from the collection. After gathering data, the literature is screened and organized according to the Artificial Intelligence methods used such as machine learning, deep learning, and federated learning—and the fields of application, including intrusion detection, authentication, anomaly detection and data privacy.

A comparative analysis framework is applied to synthesize findings, highlight similarities and differences, and critically evaluate the strengths and limitations of prior work. The following diagram shows the flow of study and every steps explained in brief.

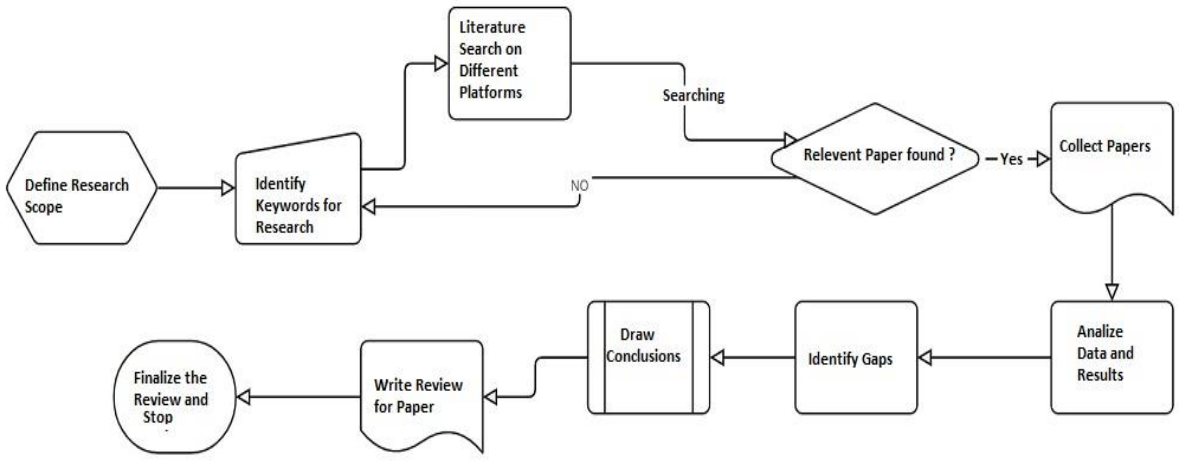


Figure 2: Steps of Research Methodology

- **Define Research Scope:** This study begins by defining the research scope with clear objectives and boundaries. Unlike conventional approaches, this study is aligning the scope with both academic relevance and emerging smart home security applications, ensuring the review remains impactful for theory and practice. The scope of study is only focusing on the

Received: August 01, 2025

Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
major threats, threats detection, classification and mitigation using AI /ML s in commonly using communication protocols specially for smart home environment.

- **Identify Keywords for Research paper searching:** Appropriate keywords are identified using both manual brainstorming and automated keyword extraction tools like Scopus indexed keywords and IEEE Thesaurus and combine the both for keyword search. This integrated approach enhances the precision of literature searches and also reducing the likelihood of missing relevant studies.
- **Literature Search on Different Platforms:** Literature is searched across multiple academic platforms such as IEEE Xplore, Scopus, Springer, and ACM, along with others open access repositories. The approach used here is in the inclusion of grey literature and preprints to capture cutting-edge trends often missed in traditional reviews using keywords "smart home" OR "intelligent home" OR "IoT home" OR "home automation") AND ("security" OR "cybersecurity" OR "privacy" OR "data protection") AND ("artificial intelligence" OR "AI" OR "machine learning" OR "deep learning" OR "federated learning" OR "reinforcement learning " OR "anomaly detection in smart home". From more than 200 papers 56 most relevant selected for further stydy.
- **Check for Relevant Papers:** Papers are screened for relevance based on title, abstract, and content alignment above mentioned keywords, year range (form 2014 to 2025) , applied approach and domain checked to increases the accuracy of paper selection.
- **Collect Papers:** Relevant papers are downloaded and organized from different online libraries or peer reviewed journals like MDPI, Springer, IEEE library, Wiley etc.
- **Analyze Data and Results:** Each paper is studied, categorized and analyzed not only for its methodology and results but also for its reproducibility, dataset usage, and scalability of findings to find the gray area of research.
- **Identify Gaps:** This study finds the research gaps by mapping findings against emerging trends and practical demands and emerging different security system approaches. The novelty in this approach is to create a structured “gap matrix” that categorizes gaps into technical, methodological, and application-specific areas.
- **Draw Conclusions:** Conclusions are drawn and reported for not just in form of summaries but as in form of strategic insights highlighting opportunities for innovation. The novel element is the formulation of forward-looking recommendations that integrate academic challenges with real-world deployment needs.
- **Prepare a paper using above findings:** The synthesized findings and conclusions are written into a review paper by following the standards of journal of reputes in a better way to enhance clarity and depth of the review.
- **Finalize the Review and Stop:** The process concludes with iterative refinement to ensure clarity, rigor, and novelty in contributions. Unlike conventional reviews, this methodology ensures the final work not only summarizes the state-of-the-art but also provides actionable insights for future researchers and practitioners.

The above research methodology is following in this study and the novelty of this research methodology lies in its systematic integration of traditional literature review steps with innovative practices such as tool-based keyword refinement, inclusion of grey literature,

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
thematic clustering of research works, and comparative benchmarking across datasets. Additionally, the structured gap matrix and forward-looking recommendations ensure that the review not only synthesizes existing knowledge but also provides practical guidance for future research and real-world applications.

4. Literature Review and related work

Initially smart home was only conceptual or ideological thing, not actual structure. The timeline of the smart home design and development is as given below [8].

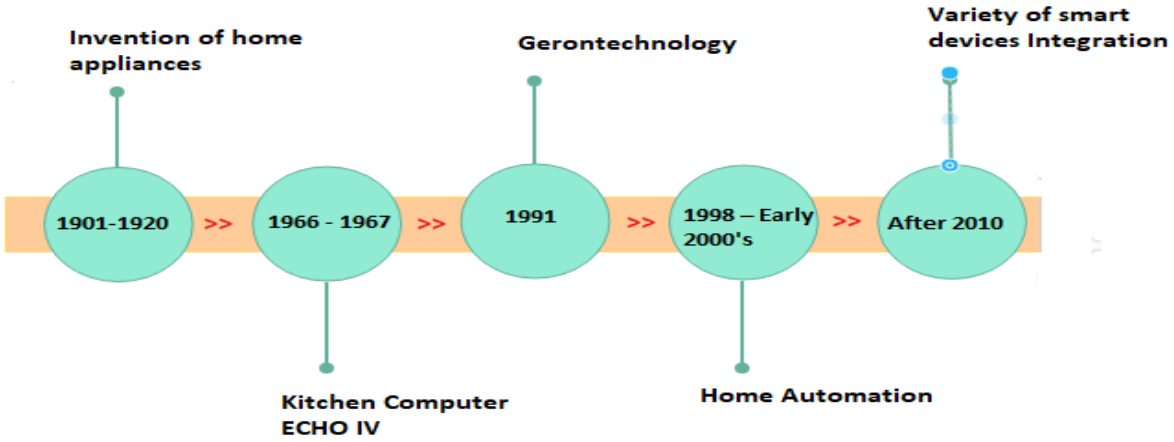


Figure 3: Evolution of Smart home devices

In early 1900: - This was the era of Invention of basic home appliances**.** The home appliances at that time were basic models and based on mechanical and electric powered not smart as what we do consider these days but these appliances were remarkable achievement in this time span. In 1901 the first engine powered vacuum cleaner was invented. The electric-powered washing machines were advertised in newspaper in year 1904 and the next version of vacuum cleaner which was electricity powered invented in year 1907.In year 1909, the successful electric toaster was introduced by General Electric and refrigerators for domestic use were invented in year 1913. Then afterward clothes dryers, electric irons, air conditioner and so much more were invented. It was really a time span of innovation and invention for the basic model of home appliances to make life more comfortable and easier.

Kitchen Computer: -The first smart home computer named Kitchen computer ECHO IV from Honeywell had developed in year 1966 and it based on 16-bits microprocessor capable to store food recipes and provides tips for cooking while preparing the food. It was also capable to manage and store shopping list and also control the humidity and temperature of home, in spite of this it was never sold commercially.

Beginning of Smart lighting system: In 1975 Pico Electronics discovered X10 Home automation project to control homes lights and small appliances using existing power cabling and launched and sold products under the X10 label.

Gerontechnology (Year 1991) – The term Gerontechnology consists of two major terms gerontology and technology, which was an early step to make the livings of senior citizens more convenient and easier. Gerontological design used to providing services to make

Received: August 01, 2025

Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
convenient way of life for senior citizens based on solutions to monitor their health, mobility pattern, way of communication, leisure and working of senior people using their concerns matching technological.

Smart Homes (1998-Early 2000's) –Home automation, smart homes and connected homes were started to acquiring the recognition in early 2000. As such, different communication technology based connected home or smart home appliance began to come in market for the integration with smart home. This made smart home became an overall cheaper option with better safety & security and full of convenience. But at that time smart homes had limited features and complex and hybrid architecture to control and communicated with these home appliances.

Current Smart Homes – In today's scenario smart homes have more safety, privacy and security environment and energy friendly features. Current situation home homes include lightening automation, automated temperature regulation, activity scheduling of appliances, remote accessibility using smart phones or web, alerts or notifications in form of mail/messages, video surveillance with remote accessibility and activity oriented, smart washing machine and biometric or code based smart locks [9]. But these devices belong to different companies and can't provide a homogeneous central device management system. In current scenario these smart devices have not true sense of data security and privacy while data in rest or under transmission to cloud systems.

In this study article's year from (2014 to early 2025) of existing protocols, IoT system, smart home security and privacy issues. As per John A [9] research directions in IoT system is very wide but the prominent areas are huge scaling of Iot network and related issues, architecture and dependency, security and privacy issues of data, robustness and openness, creating knowledge and big data etc. According to this paper there are three major challenges in such network are understanding of complete spectrum of types of human in the loop controls and need for identification or other techniques to derive the human behavior identification models.

Another is selection of secure communication protocols for smart home communication, like Bluetooth, Low energy Bluetooth [10], Zigwave, Z-Wave, Thread, WiFi, 6LowPan, NFC, Sigfox, Cellular and LoRaWan. Some of the protocols are very conventional, old and multipurpose. Some protocols are very new and special purpose and their new versions are under development phase. But every protocol has security and privacy flaw and not provides a good sense of security which may be applicable to the smart home to take real feel of security at home. And third one is to design implement a security system which watch the communication pattern and find out any identify the security attack and take appropriate major to minimize the total loss using AI/ ML.

Privacy and Security issues, vulnerabilities and threats in existing protocols for communication in smart home environment are as given below.

- Bluetooth [10]: It is a short range communication protocol working using ISM band from 2.402 to 2.48 GHZ. Bluetooth has range of 1 to 100 meter depend upon the class version and working at data link layer of IoT communication, it is suffering with, Bluesnarfing, Bluejacking, Bluebugging, Car Whispering, Denial of service securities attacks and issues. The Bluetooth

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
Low energy (BLE) [11] is better one in terms of energy efficiency but it has Man in the middle attacks, passive eavesdropping and Identity tracking security challenges.

- ZigBee [12]: It is an open standard communication protocol use for Machine to machine communication and well working with low power applications and low data transfer rate (up to 250 kbps) with short range communication from 10 meter to 100 meters. The Zigbee WPANs (Wireless personal area networks) generally operate on 868 MHz, 900MHz and 2.4 GHz frequencies. But Zigbee enabled devices has threats of Physical Attack, Key Attacks, Replay and Injection Attacks.
- Z-Wave [13]: it is a MAC layer wireless communications protocol primarily used for the smart home and commercial building automation. It works on 800-900MHz radio frequency and considered a secure and middle range communication protocol 100meters to 800 meters range with 100kbps data transmission speed. It has also other types of attacks like Black Hole attack, Impersonation attack, Outsider topology discovery etc. and these are not very often but it may harm the confidentiality and integrity of smart home network.
- 6LowPan [14]: It is a network layer protocol which stands for IPv6 over Low-Power Wireless Personal Area Networks working with low powered and mess topological network where every node has its own IP address. It is working using IEEE802.15.4 standard and using 2.4GHz radio band with 200m of range and 200kbps of data transmission rate. It can use AES encryption techniques using up to 25 bits' key size to encrypt data in 128bits block size. It doesn't support no repudiation and element-wise signing and encryption. It has transport layer security limitations while using datagram transport layer security.
- Wi-Fi [15] (Wireless Fidelity): It is a family for wireless communication protocol based on IEEE802.11 standards. Wi-Fi use to connect home appliances, phone, computers, TV etc. to internet and make life easier. It operates of 900MHz to 60GHz range depend upon version to be used, it has maximum 50 meter of range and data transfer rate is 54Mbps to 866.7 Mbps. Wi-Fi protected access (WPA) and WEP (Wired Equivalent Privacy) can cracked in minutes' bur WAP 2.0 can also be cracked but it required more time and efforts. The main data security and privacy issue with insider user which has bad intension to eavesdrop the packets under transmission from one node to another.
- Cellular [16]: Cellular network provide a way to connect physical things or home appliances using 3G, LTE, 4G and 5G network to provide mobility and higher data up to 100+ mbps average data transfer rate. The cellular network has still some set of privacy and security challenges like Bandwidth Stealing, location tracking, bandwidth stealing, security issues because of Open Architecture, Man in the middle attack, DoS Attacks. Cellular IoT enabled devices are already secure, as part of the GSMA standards but it required some additional encryption layer required to secure multilayer data security.
- Thread [17]: It is IPV6 enabled networking protocol supports IEEE802.15.4 standard wireless mess network used to connect low powered IoT devices. It is IP enabled communication protocol can be used in smart home network for seamless connectivity using 2.4 GHz radio frequency and provide interoperability with Wi-Fi and other communication protocols with

Received: August 01, 2025

Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

speed of 200Kbps and connectivity range is 30meters. It provides large scalability up to hundreds of devices with encrypted communications but thread has some security and privacy issues and vulnerabilities like physical attacks, encryption related issues as mentioned in 6LowPan, UDP services has more security and privacy vulnerabilities.

- LoRaWAN [18]: It is a low power wide area network protocols use to connect battery operated IoT devices and provides end to end security for bi-directional 128-bit encrypted communication, mobility using 169 MHz, 433 MHz (Asia), 868 MHz (Europe) 915 MHz (North America) and 2.4GHz (worldwide) bands at 0.3 kbps to 50kbps with low latency with converge range is 960meters. It has some security issues are Physical device attack, Encryption keys related issues and non-optimal encryption, Data handling trust issues on data transmitting nodes, LoRaWan gateways has security compromise issues and internet interfaced nodes are common targets for hackers.
- NFC [19]: Near Field Communication is a short-range wireless communication technology distance up-to 4 cm or less to transfer small payloads between NFC tag and NFC enabled android device with data transmission rate of 424 kbps working at 13.5 MHz frequency. It can be use in smart home for very short range communication like lock unlock doors, turn light on/off etc. It has limited uses in smart home but in spite of this it has security issues like NFC tag physical thefts, Interception Attacks, Data Corruption and Manipulation and Eavesdropping.
- Sigfox [20]: The Sigfox protocol uses ultra-narrowband 200 kHz for public use and 868 to 869 MHz and 902 to 928 MHz radio bands for message transmission over the air, these bands are depending on the reason of operation ultra-narrowband use to save energy and provide the range is about 1,000 meters for data transmission. This protocol has some major issues like limited application in smart home environment, Less volume of Data transmission (In 24 hours only 140 Uplink message of 12 bytes' size and 4 downlink messages of size 8 bytes only), Data Security issue at network layer.
- CoaP [21]: Constrained Application Protocol (CoAP) is a web enabled protocol design to connect semi intelligent and smart devices or IoT enabled nodes. It follows the client server architecture to work with constrained node in constrained network. It also supports restful API web enabled requests between client and server nodes using udp communication under datagram transport layer security. It has many security issues and vulnerabilities like Dos attacks, Relay and Replay attacks, Man-In-The-Middle Sniffing and Spoofing etc.
- MQTT [22]: Message Queuing Telemetry Transport is a light weight an, publish subscribe based model application layer protocol, use to connect IoT devices and capable to provide machine to machine communication. The sensor node or device publish the data (topics) to the server (broker) and the multiple clients subscribe the topics on the basis of received topic's data the clients actuate some action or performs some job. MQTT has security, authentication, interoperability challenges. MQTT is has some kinds of major attacks like Dos attacks on broker, man-in- the-middle attacks, replay attacks, encryption issues in-spite of TSL/ SSL security.

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Matter [23]: An Internet Protocol (IP)-based smart-home technology that seeks to provide seamless integration across multiple Internet of Things (IoT) devices, such as smart lights, switches, sensors, thermostats, and home appliances, is Matter. Matter's devices communicate through Wi-Fi (2.4/5 GHz) and Ethernet, Wi-Fi and Threads have unobstructed indoor communication ranges of Wi-Fi (30-50 meters) and Threads (10-30 meters). Google and Apple voice systems are integrated into Matter, and Matter assists in integration through standardizing device commissioning, communication models, and multi-admin support. At the same time, Matter includes privacy and security features like end-to-end encryption, device attestation and certificate-based authentication. Despite these features, and the nature of smart home technology which prioritizes privacy, it is worth noting that Matter has the same security concerns that such technology has, namely, border router vulnerabilities, compromised local networks, tampering of supply chains, and firmware update weaknesses. The range of such technology inevitably has to surpass the smart home to some extent and these factors reveal the need to deploy smart home technology that is reliable, scalable, and preserves the privacy of the home and its occupants. The following Table-1 includes the comparison of the various protocols alongside their respective smart home use case scenarios.

Table 1: comparison of the various protocols alongside their respective smart home use case scenarios

Protocol Name	Frequency	Range	Security Features	Strengths	Limitations / Weaknesses	Use Cases in Smart Home
Bluetooth / BLE	2.402–2.48 GHz	1–100 m	Basic pairing encryption, BLE energy-efficient security	Low power, widely supported, easy device pairing	Bluesnarfing, Bluejacking, Bluebugging, MITM attacks, eavesdropping	Wearables, smart locks, short-range sensors
ZigBee	868 MHz, 900 MHz, 2.4 GHz	10–100 m	AES-128 encryption	Low power, mesh networking, robust M2M communication	Physical attacks, key attacks, replay/injection attacks	Smart lighting, switches, sensors, automation
Z-Wave	800–900 MHz	100–800 m	AES-128 security, secure inclusion	Low interference, long range, good reliability	Black hole, impersonation, topology discovery attacks	Door locks, thermostats, building automation
6LoWPAN	2.4 GHz (IEEE 802.15.4)	~200 m	AES encryption (up to 128-bit blocks)	IPv6 support, low power mesh, scalability	No non-repudiation, weak DTLS support, transport-layer issues	Energy-efficient sensors, IPv6-based smart devices
Wi-Fi (802.11)	900 MHz–60 GHz (variant dependent)	~50 m	WPA2/WPA3 authentication & encryption	High data rate, existing home infrastructure	Insider eavesdropping,	Cameras, appliances, high-

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

					WEP/WPA vulnerabilities	bandwidth devices
Cellular (3G/4G/5G)	Licensed bands (various)	Wide area (cell-based)	SIM-based authentication, GSMA security	High speed, mobility, wide coverage	MITM, DoS, location tracking, bandwidth theft	Remote monitoring, outdoor devices, mobile IoT
Thread	2.4 GHz (IEEE 802.15.4)	~30 m	Encrypted IPv6 mesh, secure commissioning	Low power, scalable mesh, high interoperability	Physical attacks, UDP-based vulnerabilities, encryption challenges	Smart sensors, home automation clusters
LoRaWAN	169/433/868/915 MHz, 2.4 GHz	~960 m	End-to-end AES-128 encryption	Long range, low power, scalable	Key mismanagement, weak encryption setups, gateway compromises	Outdoor sensors, long-range utility monitoring
NFC	13.56 MHz	≤ 4 cm	Short-range secure pairing	Very low power, simple tap-based operation	Physical theft, interception, data corruption, eavesdropping	Smart locks, access control, device pairing
Sigfox	868–928 MHz (UNB 200 kHz)	~1,000 m	Basic network-layer security	Ultra-low power, long range	Very low data rate, few daily messages, network-level vulnerabilities	Remote meters, simple status sensors
CoAP	App-layer over UDP (various physical layers)	Depends on underlying layer	DTLS-based protection	Lightweight, RESTful, ideal for constrained devices	DoS, relay/replay, MITM, spoofing	Lightweight control signals, constrained smart devices
MQTT	App-layer over TCP/IP (various physical layers)	Depends on network	TLS/SSL (optional), auth plugins	Lightweight, scalable pub/sub, efficient for sensors	Broker DoS, MITM, replay, weak default encryption	Sensor networks, event-driven automation
Matter	Wi-Fi (2.4/5 GHz), Thread (2.4 GHz), Ethernet	Wi-Fi: 30–50 m; Thread: 10–30 m	End-to-end encryption, device attestation, secure onboarding	High interoperability, multi-admin support, unified ecosystem	Border router risks, firmware security, local attack vectors	Lighting, appliances, sensors, multi-brand automation

Dimitris Geneiatakis et al. [24] proposed and setup the scene for a privacy and security threat analysis for a smart home architecture using off the shelf components. To achieve the same,

Received: August 01, 2025

Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
they utilize a smart home IoT architecture that enables users to interact with it through various devices that support smart house management, and analyze different scenarios to identify possible security and privacy issues for users. This approach provides a scene and real feel of security and privacy threat analysis for a typical smart home architecture that relies on existing and readily available market IoT devices and platforms. In this study the authors leaved a grey line for the integration of a framework for the risk analysis of the prominent threats.

Aimin Yang Et al. [25] described the major aspects of security and privacy issues of IoT system and integral design of Smart homes, and proposed and designed an intelligent video surveillance based on stereo matching algorithm by which a home owner or smart home system can classify the data in real time or no real time based on binocular stereo matching with multiple view points and the author tested and find out improved performance of matching degree only in Wi-Fi network.

Khushal Shingala, Jignesh Patel [26], discussed and proposed a smart home computerization web enabled framework which uses SMS, mail system, and home appliance control system with secure environment within the smart home. This framework provides the controls on home appliances remotely and gives a real sense of security especially when client is far from home. The proposed algorithm uses the different sensors (like PIR sensor, MQ5 Gas sensor, electromagnetic door sensors, temperature sensor etc.) and their states and their composition value to analyze the situation of internal environment of home and transmitting the alerts to the home owner based on SMS and email. There are many scope in this paper for improvements.

Vaishnavi S. Gunge and Pratibha S. Yalagi [27] well explained the smart home automation and literature review of sixteen papers and they discussed the challenges of Home automation like high manufacturing, development, support and maintenance cost, lack of home automation standards, complex user interface etc. Their paper provided a well explanation of WiFi and Zigbee based home automation and monitoring system, cloud based home appliances monitoring and controlling system designed to collect the data on cloud and analyzed using map-reduce based application then provide insight and control to remote user. This paper also provides the comparison among different kinds of home automation system, their communication interface, controller hardware, user interface, Application and its benefits.

J. Bugeja et al. [28] about the smart connected homes a privacy centric models presented, which author explained the different components of smart connected homes like connected home is a set of smart houses, nodes, users, links, data, privacy policy and safety attributes and provides the enumeration and analyze the IoT privacy threats based on biometric identifiers location, MAC addresses of connected devices, user operation and read write permissions. Authors also proposed and explained a smart connected home setup consisting of three connected devices – smart speaker, video doorbell, and smart lock; mobile device – smart phone and a cloud endpoint. This configuration allows the homeowner the possibility to unlock a door using his or her voice as input and remotely through a smart phone. This only an empirical and explanatory study required many improvements in terms of real time decisions and risk assessment model.

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
S. Nagarkar et al. [29] in his survey paper well described the importance of privacy in smart home to protect the personal information, identity, movement, live location etc. of user. This paper also discussed the data privacy, context aware privacy and security issues in the smart homes in biometric identification systems, RFID enabled key and access cards for the access controls. This paper also explained the six objective of smart home environment- Confidentiality, Availability, Integrity, and Authentication, Authorization and Non-repudiation and their ways to maintain. The author also explained the security and privacy vulnerability due to many reasons like wireless protocol issues, heterogeneity and compatibility of IoT devices to communication technology, low computational power of controllers, integration and cloud storage security issues, weak authentication mechanism and fixed firmware of IoT devices. This paper also discussed the counter measures for the smart homes after face to face interviews of 92 smart home users, the key points of that interview are awareness and training need for better uses of technology, issues of securing home network, application of intrusion detection system, issues of data backups and encryption techniques etc.

The research published by F. Liang et al. [30] highlighted the use of Machine Learning (ML) technologies in cybersecurity and cyber-physical systems (CPS)/Internet of Things (IoT) technologies and discussed advantages, disadvantages, and the issues of greatest concern. The authors discussed in detail the numerous advantages that ML technologies offer in the field of security and in CPS/IoT, including advancements in Intrusion Detection Systems (IDS) and improved decision-making within CPS/IoT environments. The authors also examined the disadvantages of ML in the security, CPS, and IoT domains, in particular the vulnerabilities of ML systems to manipulation and exploitation at every stage of their life cycles, from data collection to validation and deployment. One major concern was the use of ML to automate cyberattacks and intrusions, which represents a poorly understood and potentially damaging application, or "ugly" use of ML in these situations.

E. Anthi et al. [31] well explained the importance of IoT and its application, range of attacks in IoT environment like data leakage, spoofing, disruption of service (DoS/DDoS), energy bleeding, insecure gateways, etc. Authors proposed an intrusion detection system with supervised machine learning techniques for classification for three purpose (1) device type classification, (2) malicious packet detection classification, and (3) attack type classification. This paper used the classification algorithm using decision tree and for the feature space is relatively large, all packet features may not be relevant. Two main feature selection methods were used to identify the most relevant features; Correlation Attribute Evaluation Filter and Gain Ratio Attribute Evaluation Filter. The author also discussed the result of his experiment that reports the overall weighted-average performance for all 9 classifiers, including their classification time. Overall, Weka's implementation of J48 decision tree method with pruning achieved the best performance, resulting in an F-measure of 99.7%, 97.0%, and 99.0% and a classification time of 0.1 seconds, 0.4 seconds, and 0.2 seconds for each experiment respectively. In this research paper all study is given a he positive findings of the initial study, but the system is not implemented real time. So there is a lot of scope is available in this area for improvement and we can take consideration smart home security and privacy for research topic.

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
In the study conducted by Cui, L. et al. [32], a thorough examination was presented, elucidating the latest advancements in Machine Learning (ML) techniques tailored for the Internet of Things (IoT). The paper not only offered insights into a multitude of IoT use cases but also provided a comprehensive overview of how ML is applied to enable users to access profound data analytics capabilities and create highly efficient and intelligent IoT applications. Within the paper, several key topics were explored, encompassing traffic profiling, the identification of IoT devices, security measures, the architectural aspects of edge computing, network management strategies, as well as prevalent IoT applications. Additionally, the study addressed existing unresolved issues and research challenges within this domain, making it a valuable resource for those interested in the intersection of ML and IoT.

Soumya Kanti Datta et al [33] presented and explain anomaly detection model for smart home in which two types of data collection done in first researchers collected the user activity data and sensor data which is generally called behavioral data (from different appliances) and second is network data which refers to the TCP/UDP packet data from IoT devices. In this paper researchers used the HMM (hidden markov model) to learn the common behavior of smart home. To train and test the learning model authors used 780 records. 70% of data used for train the system and rest for validate the system and set the threshold value is 7 (ALP score range was 1 to 7). To evaluate the model's ability to detect abnormalities, authors manually generated a few anomalous scenarios that can happen with the sensors present in the current smart home. Like Stove On with user not present in the home etc. After this experiment authors got 97 % accuracy but they left the scope of study when data set is huge and study can be done more efficiently with other machine learning algorithms.

Faisal Alghayadh and Debatosh Debnat [34] well explained the security threats, issues, types of attacks in smart home network and introduce a two tiered IDS (Intrusion detection system) for the better security and protection in smart home network. The first tier of tis HID (Hybrid intrusion deletion system) this paper use Random forest model for finding the unusual activity in the communication network and second algorithm use to scan the user profile and user's behavior profile for misuse detection. This paper only tells only about the proposal and not show any real implementation. This research can be extended for the better result and use of multitier or multilevel ML algorithm for pattern findings for better safety and security in smart home.

N. Elsayed et al [35] explained the IoT based home devices like video doorbells, Google Homes, Wify cameras etc and also proposed and explained a novel instruction detection system for smart home which uses BiLSTM (bidirectional long short-term memory) and CNN (convolutional neural network) hybrid model. This model uses a dataset with only 42 rows from IEEE Data Port to trained and test the model. And find a good accuracy, F1score and precision (98%) This result may improve with mare large dataset.

E. D. Alalade et al [36] discussed an instruction detection system implemented with the help of AIS-ELM (Extreme Learning Machine and Artificial Immune System) which uses clonal algorithm and ELM for optimization of Input and identification of anomalous activity

Received: August 01, 2025

Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
respectively. This paper disused the proposed algorithm in form of flowchart and pseudocode only but not discussed any implementation which can considered as further extend the work.

Meidan et al. [37] introduced CADeSH, a collaborative anomaly detection framework for smart homes that leverages auto encoders with clustering to identify malicious traffic in consumer IoT networks. Using a 21-day dataset of traffic from multiple devices with injected attacks, the system achieved high detection accuracy (macro AUPRC 0.841, F1 0.929) while reducing false positives, and the dataset was released to support reproducibility.

Majib et al. [38] developed FRIoT specialized security system to support anomaly detection and activity recognition, this study implemented a multimodal dataset capturing appliance power usage, motion, and environmental sensor data. FRIoT was designed with more than 5,000 hours of annotated traces, and it directly addresses the lack of real-world smart home datasets and serves as a benchmark resource for AI and machine learning evaluations.

Manandhar et al. [39] performed a large-scale empirical study which involved 2,442 devices from 596 different vendors. The study examined smart home device privacy policies and their compliance. The study found a disturbing pattern of inconsistency, incompleteness, and inaccessibility of privacy policies which highlighted a lack of transparency. The dataset and study scripts were provided for further research and auditing purposes. Furthermore, this study train and test 3 machine learning models spaCy (baseline), PolicyLint, PolicyLintHome for named entity reorganization, recognition of data objects and entities with maximum 79.39%, 82.38%, and 80.86% precision, recall and F-1score,

Zavalyshyn et al. [40] produced a Systematization of Knowledge (SoK) that classifies privacy-enhancing smart home hub designs. Reviewing over 37 papers and prototypes, they outlined design taxonomies involving manufacturer usage descriptions (MUD), data minimization techniques, and gateway mediation, while highlighting usability and deployment gaps. This study discussed the aspects that in now a days cloud-centric models continue to dominate smart home systems, but there is a noticeable shift toward hub-based and hybrid architectures that enhance privacy through local data processing and data minimization techniques. These findings offer critical guidance for developers while opening new directions for research on privacy-preserving technologies in smart home environments.

Xuan Dai et al. [41] introduced HomeGuardian, a context-aware anomaly detection framework that combines statistical modeling with machine learning to identify abnormal events in smart homes. HomeGuardian was tested on a set of sensor and activity logs and it demonstrated a notable reduction of false positives when compared to legacy techniques, all the while preserving the high usability standard set for smart home systems. The HomeGuardian uses a ML based classifier to predict the normal or abnormal event on event data for the context aware smart home system and good f1-score value beyond the 90%.

A. Chatterjee [42] provided a detailed overview of the various approaches for detecting anomalies in the Internet of Things (IoT) systems, which ranged from supervision, unsupervised, and deep learning approaches. The literature review underscored the limitations of available datasets, the challenges posed by concept drift, and the constraints imposed by the

Received: August 01, 2025

resources available on the devices, and provided a taxonomy for the selection of appropriate anomaly detection approaches for smart homes.

Samiul Alam et al. [43] released FedAIoT, a benchmark repository to standardize federated learning evaluation in AIoT, including smart home environments. The framework incorporates eight datasets, baseline models, and partitioning scripts to simulate non-IID client distributions, enabling reproducible FL research for IoT security. This study used multiple dataset like WISDM, CASAS, AEP etc to train multiple ML based models like LSTM, CNN, 5 layer MLP, SVM, liner regression, GRU, Yolo and achieve maximum accuracy of 95% in case of UT-HAR data set in case of centralized learning.

Zhang et al. [44] proposed FedGroup, a federated anomaly detection approach for IoT that groups clients based on similarity to mitigate data distribution issues of conventional machine learning techniques. Experiments on multiple smart home datasets demonstrated that FedGroup improved both detection accuracy and privacy preservation compared to standard FL methods. The research explained and implemented a set of Federated learning based models like FedGroup, FedAvg_EL, and FedGroup_EL to enhance anomaly detection accuracy for smart home IoT systems. The experiment's result shows that federated learning using ensemble models attains accuracy levels exceeding 99% and surpasses the conventional ML models on the dimensions of fairness, fault tolerance, and robustness. Such approach optimally try to mitigate privacy and security risks, and facilitate future inquiries concerning the learning in real-time and the cost of the system in the federated arrangement.
Sujit Biswas et al. [45] Developed a federated learning framework for smart home security that is augmented with blockchain technology, with the aim of building trust in provenance and model aggregation. The research used energy consumption datasets to show how the integration of blockchain technology in smart homes, despite of the processing and communication overhead, can consider as a secure model updates. This study achieved 88% validation accuracy, about 30% higher than standard ML, and improves further in testing where the 50th global model classifies 86% of images correctly. These results highlight that the distributed FL-based approach not only outperforms traditional ML but also strengthens scalability, security, and privacy in smart home networks.

Vanen et al. [46] designed a multi-layered id (intrusion detection system) with a home environment in mind. This system conducts packet analysis in conjunction with several types of ML classifiers. Their work, conducted on TCP/IP dataset from Kaggle.com, demonstrated not only higher detection rates than conventional methods, but also evidenced how feature selection and various ML classifiers, such as the Naive Bayes Classifier, Decision Tree, KNN, and Logistic Regression used for binary classification with respective accuracies of 90.7%, 99.6%, 099.4%, and 95.5%, helped in achieving a considerable reduction in the number of false positives.
S. Sohail et al. [47] proposed and implement an optimally configured Artificial Neural Network (ANN) for identifying attacks in the smart home domain. Their work produced exceptional results in the range of 99.9% accuracy for the binary classification problem, 99.7% accuracy for the category-level detection task, and 97.7% accuracy for the subcategory-level classification challenge. They have all the time focused on explainability and have fine-tuned

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
hyperparameters which lead high to precision as well as turn the system into a transparent one. Thus, they have solved one of the crucial problems of ML-based smart home security systems.

Aljabri et al. [48] have developed an IoT intrusion detection system referring to only the use of supervised machine learning techniques for the detection of Flood and Brute-Force attacks detection. They have executed their Gradient Boosting classifier with 95.9% of accuracy using six features and 95.3% of accuracy with only three features. This study is especially significant for smart home devices at the edge where computational resources and memory are limited because it has been proved to be capable of still ensuring high detection accuracy when the feature input is minimal.

Farea and Kucuk [49] proposed IDPS (hybrid Intrusion Detection and Prevention System) machine learning-based intrusion detection system for edge-based Industrial IoT (IIoT) applications, which is highly applicable to smart home environments. Using KoU-6LoWPAN-IoT and Edge IIoT datasets, their system achieved binary classification accuracy up to 99.9% and, and multi-class classification accuracy of 95.65% accuracy using ANN classifier. This paper uses the classifiers like Decision Trees highlights the system's feasibility for edge deployment, which offering a favorable trade-off between computational efficiency and classification performance.

Aldaej et al. [50] introduced a deep learning-based intrusion detection system for IoT deployed in edge–cloud environments. The approach begins by partitioning the large BoT-IoT time-series dataset according to attack types and then applying feature selection to aggressively reduce dimensionality—cutting the number of attributes by around 85%—without sacrificing model performance. This paper trained hybrid models like Random Forest, SVM, RNN and Bi-LSTM layers on this cleaned dataset. Models of this study delivered outstanding results up to: 99.56% accuracy, 99.45% precision, 98.25% recall, and a 99.12% F1-score for RNN classifier. This demonstrates that intelligent feature selection not only helps meet edge-device resource constraints but also maintains, or even improves, high detection performance in real-time IoT security applications.

Federated learning, blockchain and data distillation are the techniques described by Shalan et al (2025)[51] to detect a bot attack in a smart-home IDS. The proposed system allows IoT devices to collaboratively train while maintaining privacy, knowledge distillation reduces the computation required on weak devices, and blockchain enforces role-based access control, ensuring only authorized devices contribute. The N-Bait dataset used in this study and, achieved 91% of accuracy matrix for anomaly-detection for botnet attacks while preserving system integrity. However, integrating blockchain introduces extra latency and computational overhead, and knowledge distillation may result in some loss of model fidelity under certain conditions.

Ansam Khraisat et al. (2025) [52] compares the basic Federated Averaging (FedAvg) algorithm to a more complex, modified version referred to as FedAvgM, on a series of IoT devices. The study mentions the PEIoT-DS system which incorporates federated learning to build an IDS model without the need to share data. The system evaluation done on the N-Bait dataset confirms good detection accuracy while protecting data privacy. Nevertheless, the

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
authors note that communication overhead and real-world deployment on highly constrained devices remain practical challenges.

Wankhede and Patel [53] describe an integrated federated learning and blockchain architecture ("FL- BlockIoT") designed to protect IoT data aggregation. With their design, and through the use of federated learning to remove the raw data from the iterative process, user privacy is maintained and tampering is prevented as model updates are logged and then blockchain-anchored. The framework targets distributed trust among edge devices, but the paper acknowledges a trade-off: blockchain consensus mechanisms induce latency and resource usage, which may limit the system's feasibility in real-time or resource-constrained smart home environments.

Deshmukh et al. [54] investigate a federated-learning-based IDS for intrusion and fraud detection in IoT-enabled infrastructure. Using the Flower framework, each device trains locally and contributes to a collective model, preserving data privacy. The absence of sensitive data from the testbed is a positive feature of their detection strategy, especially when privacy is of high concern. The absence of data is, of course, the Achilles heel of all simulated testbeds. Therefore, design weaknesses are also likely to be predominantly untested. The design has not assessed its ability to withstand the rigors of a real live test, especially when the devices used in the testbed are diverse and the networks are unsteady.

Kumar et al. [55] describes a blockchain IDS, built using a modular approach, to integrate lightweight cryptography, and the SHAP (SHapley Additive Explanations) method of explainable AI. The explainable nature of the decisions that the IDS makes provides immutable proof of the trust that can be placed in that decision, with model updates stored in the blockchain, retaining the benefits of decentralization. The design strikes an impressive balance of transparency, system resilience, and explanation of trust, but the authors note that meeting the design intent of low latency and low resource use could be problematic, given the constraints of blockchain and SHAP.

Rahmati (2025) [56] worked on an anomaly detection approach with homomorphic encryption model fusion. Federated Learning-Driven Cybersecurity Framework for IoT serves DDoS attacks. Achieving a detection rate of more than 98%, this design allows decentralized data training and retention of raw data, along with model privacy. The study also claims more efficient energy use than centralization. However, because it's evaluated in a controlled simulation, the framework's performance under real-world edge scenarios including network unreliability and very constrained devices remains to be demonstrated.

To better understand the evolution of smart home background, communication protocols and security mechanisms, a comprehensive literature review was conducted covering key studies from 2014 to 2025. The reference from [1] to [9] used to explain the background of smart home and its related technologies, form [10]-[22] discussed about used communication protocols and it's shortcoming form [22]- [35] references focused on security attacks, different approaches to handle them using different AI and ML algorithm, Hybrid AI based models with small datasets , and reference from [36] to [56] used multiple statistical approaches , AI-driven approaches with moderate and large size of data sets for to make smart home more secure. Table-1 presents

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
a comparative summary of nineteen selected research works [36]– [56] that collectively span privacy-preserving architectures, intrusion detection systems (IDS), anomaly detection models, and AI-driven approaches for IoT-based smart homes. The reviewed studies employ a wide range of techniques—including Random forest model, KNN, SVM, ANN, Hidden Markov Models (HMM), hybrid machine learning frameworks, deep learning architectures (CNN, LSTM, DNN), blockchain and federated learning to address the challenges of detecting and mitigating cyber threats in heterogeneous IoT ecosystems. While early works primarily focused on conceptual frameworks and low-cost automation prototypes. More recent contributions or studies are focusing on the integration of explainable AI and optimized deep learning models with impressive accuracy and interpretability. This comparative analysis highlights the research transition from traditional security frameworks toward intelligent, adaptive, and centered IDS solutions for smart home networks.

Table-2: Comparative Summary of AI- ML- FL -Based recent papers of this study

Authors / Year	Title of Paper	Focus Area	AI / ML / Other Techniques	Dataset / Setup	Key Findings / Contributions	Limitations / Gaps	Reference
Y. Meidan et al. / 2023 CADeSH:	Collaborative Anomaly Detection for Smart Homes	Collaborative anomaly detection for consumer IoT traffic	Autoencoder and clustering under unsupervised feature pooling	CADeSH dataset — 21 days real-world IoT traffic from 8 devices; lab attack injections	Included a collaborative techniques of Machine learning and Two-step auto encoder and clustering reduces FPR; reported macro AUPRC 0.841, F1 0.929; dataset released for reproducibility.	Only evaluated in simulated settings, limited device diversity, lacks deployment validation and scalability testing.	[37]
Y. Majib et al. / 2023	Dataset for cyber–physical anomaly detection in smart homes (FRIoT)	Dataset resource for multi-modal anomaly detection	(dataset paper)	FRIoT dataset — appliance-level power, motion, environmental sensors; 5000+ hours	Provides annotated multi-modal traces for anomaly detection and activity recognition benchmark tasks and addresses dataset scarcity and data fusion	Dataset coverage is limited to specific attack types , it does not fully represent real user behaviour and may not generalize across heterogeneou	[38]

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

					and anomaly simulation	s smart homes.	
S. Manandhar et al. / 2022	Smart Home Privacy Policies Demystified	Empirical analysis of privacy policies for smart-home vendors/devices	Empirical methods like spaCy (baseline), PolicyLint (crawling, manual coding)	Privacy policy corpus: 2442 devices, 596 vendors (USENIX dataset)	Large-scale analysis showing poor availability and inconsistencies in privacy policies; provides dataset and scripts for replication.	Focuses mainly on privacy policy analysis, does not propose or validate countermeasures and lacks empirical security evaluation.	[39]
I. Zavalyshyn et al. / 2022	SoK: Privacy-enhancing Smart Home Hubs	Systematization of hub-based privacy solutions	SoK and threat modeling in smart home	Survey corpus: 37+ privacy/hub papers and prototypes	Taxonomy of hub designs, MUD usage, data minimization strategies; discusses deployment and usability gaps.	Primarily taxonomy and conceptual analysis, real-world performance, latency, and interoperability concerns not validated.	[40]
Xuan Dai ,Jian Mao et al. / 2022	HomeGuardian: Detecting Anomaly Events in Smart Home Systems	Context-aware anomaly detection for activity anomalies	Statistical modeling + ML context models (Dynamic time warping algorithm)	HH114 dataset from CASAS	Context modelling reduces false positives; demonstrates improved detection while maintaining usability and reported f1-score value beyond the 90%.	Limited anomaly coverage, may generate false positives and dependency on controlled environment datasets reduces robustness.	[41]
A. Chatterjee / 2022	IoT anomaly detection methods and applications: A survey	Survey of anomaly detection in IoT and smart homes	Survey (ML/DL/statistical methods reviewed)	Review of multiple datasets and testbeds	Provides taxonomy of methods, highlights dataset realism and concept drift challenges, also disucssed useful reference for method selection.	Lacks implementation results and survey scope focuses on conceptual understanding rather than practical deployment constraints.	[42]

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Samiul Alam ,Tuo Zhang,Tiantian Feng et al.	FedAIoT: A Federated Learning Benchmark for AIoT	Benchmarking FL for AIoT including smart-home sensors	Federated learning benchmarks and baselines	WISDM, CASAS, AEP etc data sets	Standardizes FL evaluation on IoT data, includes partition scripts for simulating non-IID clients and reported accuracy up to 95%	Early benchmark version, high communication costs ,limited exploration of privacy leaks and hardware constraints in edge devices.	[43]
Y. Zhang et al. / 2023	Privacy-Aware Anomaly Detection in IoT Environments (FedGroup)	Federated anomaly detection with grouping strategy	Federated Learning (FedGroup) + personalization	Evaluated on public 10 IoT/smart-home device network data set for attack detection	Grouping clients improves privacy-utility trade-offs and handles non-IID behavior; better detection vs vanilla FL and reported 99.9% of accuracy on attack detection	Tested in constrained environments, model scalability, energy overhead, and defence against adversarial attacks not extensively evaluated.	[44]
S. Biswas / 2024	Blockchain controlled trustworthy federated learning platform for smart homes	FL + blockchain for trust & provenance	DNN + FL + blockchain ledger	Experiments using Kaggle energy dataset (simulated SH nodes)	Blockchain provides tamper-evidence for model updates; discusses overheads and feasibility in SH contexts and achieve 88% of classification accuracy	Blockchain integration increases latency and resource usage, deployment on low-power devices not optimized.	[45]
S. M. Vanen et al. / 2025	An Improved Intrusion Detection Scheme in a Smart Home Environment (Int. J. Computer Applications 2025)	Improved IDS scheme for modern smart homes	Proposed enhancements to IDS architecture/algorithms (used Naive Bayes Classifier, Decision Tree, KNN, LR individually)	Experimental/analytical evaluation reported in article	Claims improved detection accuracy up to 99.4% KNN practical considerations for contemporar	Results obtained with small-scale dataset, lacks consideration of dynamic attack patterns and heterogeneou	[46]

Received: August 01, 2025

					y deployments ..	s device protocols.	
S. Sohail, Z. Fan et al. / 2022	Explainable and optimally configured artificial neural networks for attack detection in smart homes (arXiv 2022)	Explainable AI for attack detection and ANN hyperparameter optimization	ANN models	Evaluated on IoT/smart-home attack datasets (as per preprint)	Demonstrates explain-ability methods and optimized ANN configurations that retain high detection performance while improving interpretability. and reported accuracy of 99.7 % in binary classification	High computational cost for real-time implementation, explainability limited to specific ANN configurations.	[47]
M. Aljabri, A.Shaahid, F. Alnasser et al. / 2024	IoT Attacks Detection Using Supervised Machine Learning Techniques (HighTech and Innovation Journal 2024)	Comparative study of supervised ML techniques for IoT attack detection	Supervised classifiers (various algorithms) evaluated and compared	Experimental datasets and simulations reported in paper	Presents comparative performance of multiple supervised learners and recommends suitable classifiers for different attack types and reported 95.9 % accuracy with Gradient Boosting classifier.	Supervised models depend on labelled datasets, struggle with zero-day attacks and evaluation lacks real-world deployment metrics.	[48]
A. H. Farea, K. Kucuk / 2024	Machine Learning-based Intrusion Detection Technique for IoT: Simulation with Cooja (IJCNIS 2024)	ML-based IDS validated through network simulation	Supervised ML techniques	KoU-6LoWPAN-IoT and Edge IIoT datasets	Shows feasibility of training and evaluating ML IDS using realistic network simulators and provides performance benchmarks and reported accuracy upto 95.65%	Evaluation limited to simulation, lacks real hardware testing and scalability issues not addressed.	[49]

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A. Aldaej, T. A. Ahanger, I. Ullah / 2023	Deep Learning-Inspired IoT-IDS Mechanism for Edge Computing Environments (Sensors 2023)	SL, DL-based intrusion detection optimized for edge deployment	Random Forest, SVM, RNN and Bi-LSTM layers	Edge-based testbed / experimental evaluation reported	Demonstrates that DL-inspired IDS can be adapted for edge computing with attention to resource constraints and reported 99.56% accuracy, 99.45% precision, 98.25% recall, and a 99.12% F1-score for RNN classifier	Edge deployment remains resource-intensive, model explainability not considered and focus mainly on detection accuracy.	[50]
M. Shalan, M. R. Hasan, Y. Bai, and J. Li (2025)	Enhancing Smart Home Security: Blockchain-Enabled Federated Learning with Knowledge Distillation for Intrusion Detection	Smart home intrusion detection with privacy-preserving learning	Federated Learning, Knowledge Distillation, Blockchain security	Federated IoT environment simulation	Demonstrates strong attack detection with improved privacy and reduced communication overhead	Scalability in highly so maintaining heterogeneous device networks remains a challenge. And required more computational power	[51]
A. Khraisat, A. Alazab **et al.** (2025)	Federated Learning for Intrusion Detection in IoT Environments: A Privacy-Preserving Strategy	Privacy-aware anomaly and intrusion detection	Federated Learning (supervised models)	IoT network traffic datasets	Reduces centralized data exposure while maintaining high accuracy	Performance decreases when device data distribution is highly imbalanced	[52]
S. B. Wankhede and D. Patel (2025)	Federated Learning and Blockchain Approach for Securing IoT Data	Decentralized IoT data security	Federated Learning + Blockchain	Experimental validation in simulated network	Offers tamper-proof distributed training with trust validation among devices	Computational overhead limits adoption in low-power IoT devices and need more computation power	[53]
A. Deshmukh,	Enhancing Privacy in	Privacy-preserving	Federated Learning (IDS +	Multi-domain datasets including	Improves detection	Lack of IoT-specific real-	[54]

P. E. de la Rosa, R. V. Rodriguez, and S. Dasari (2025)	IoT-Enabled Digital Infrastructure : Evaluating Federated Learning for Intrusion and Fraud Detection	detection for cyber and fraud threats	fraud detection models)	IoT behavioural logs	accuracy while preserving sensitive user data	time deployment testing in diverse home environments	
Atul Kumar, B. Sharma, and A. Noonia (2025)	Secure Blockchain-Based Intrusion Detection for IoT Networks	Secure IoT intrusion detection architecture	Blockchain-based distributed IDS	Simulated IoT network using smart contract integrations	Enhances traceability and trust in alert verification	Energy consumption and latency increased due to blockchain operations	[55]

The development of smart homes propagated through a range of innovations from simple electrically powered appliances to fully automated smart devices environments with interlinked network systems. These systems ranges from smart lighting, climate control, surveillance, access control etc. and these devices can be controlled and managed remotely. In relation to this rapid technological advancement, there is a growing number of Internet of Things (IoT) devices with varying communication protocols. These devices can connect using Bluetooth, ZigBee, Z-Wave, Wi-Fi, and MQTT which provide diverse challenges around privacy and security. In the last ten years (2014- early 2025) and still currently, the use of AI and ML techniques seeks to mitigate these challenges and risks through the use of HMM, Random Forest, KNN, SVM, ANN, CNN, BiLSTM, hybrid models etc., and these models aimed for federated learning. Current research has shifted towards edge devices with a focus on explainability and privacy that optimizes intrusion and anomaly detection with a focus on reducing false positives. The evolution from basic and small-scale protective measures toward smart systems that are intelligent, flexible, and privacy-ensuring is summarized in Table 2 with the cited works [36]-[55].

5. Research Gap and Research Questions

Despite significant advancements in smart home technologies, there remains a critical gap in the application of artificial intelligence (AI) and machine learning (ML) for real-time, data and communication security as well as privacy preservation. Current smart home systems employ various communication protocols and IoT architectures, but most lack in data security and privacy and integrated AI/ML frameworks capable of monitoring heterogeneous networks efficiently. Existing works are focusing on single-device security, small-scale datasets, or specific attack types, leaving challenges in multi-modal data analysis, edge-computing optimization, and context-aware decision-making largely unaddressed. Moreover, while some studies implement hybrid AI models or federated learning, but further research can be done for better attack detection, classification with optimum accuracy, privacy, computational efficiency, and explainability can be done using integrated AI, ML and FL models which remains an open research issue. A significant research gap in smart home security and privacy

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
preservation lies in developing lightweight, adaptive and explainable AI and integrated or hybrid machine learning frameworks particularly decentralize learning mechanism like federated learning models or some multilayered ML approaches that can offer robust anomaly detection and threat prevention in smart home communication network or access the device component uses. But federated learning approaches are resource intensive and user privacy and data security is major concern to interconnected home environments. In nutshell following are the major research gaps are there.

a) **Lack of Standardized or unified Security Frameworks for Smart Homes**: Despite many studies done on smart home vulnerabilities, but there is no unified, industry-accepted security or privacy framework that integrates device-level, network-level, and cloud-level risks.

b) **Insufficient Evaluation of Real-World Smart Home Environments**: Most researches are based on simulations rather than real multi-vendor smart homes or diverse type of communication protocols, where interoperability and multiple protocol's communications significantly increase vulnerabilities.

c) **Limited studies on Data Privacy**: Current studies not adequately address privacy leaks throughout the entire data lifecycle, including data collection, storage, cloud transmission, analytics, and third-party integrations.

d) **AI/ML/FD Security Models integration issues:** Existing AI/ML-based single model based intrusion detection system. These are not taking advantages of integrated approach, which uses multiple models to take unified decision for attack, and also leaving a gap for lightweight and privacy-preserving models. Federated learning and block chains has multiple issues related to data sharing and latency issues.

e) **Inadequate Study of User Behavior related vulnerabilities:** Technical vulnerabilities are widely studied, but human errors such as weak passwords, misconfigurations, and low awareness remain understudied despite being major causes of breaches.

AI, ML and federated learning driven security and anomaly detection systems are promising against evolving threats detection and classification, but real-time attack detection, model robustness for different attacks, scalability are hindered by high computational overhead and integration challenges with heterogeneous IoT devices, different communication protocols, and ensemble and hybrid learning models for enhancing privacy and security. These models are not yet widely deployed due to complexity in collaborative learning, model accuracy, and latency issues so area is very open to answer

for following research questions.

a) How can AI and ML algorithms be optimized for real-time anomaly and intrusion detection in heterogeneous smart home networks?

b) How can AI and ML algorithms be implemented for attack identification and classification on the basis of devices component uses and their communication metadata?

c) What hybrid AI/ML models (e.g., deep learning combined with classical machine learning) can improve both security and privacy while maintaining computational efficiency at the edge?

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

d) How can distributed AI approaches like FL be effectively implemented in smart homes to enhance privacy and security preserving across multiple devices?

e) What kinds of strategies can be used to integrate context-aware and behavior-driven intelligence using AI/ML frameworks for adaptive decision-making in smart home environments?

f) How can large-scale and multi-modal datasets using sensor, network Meta data, and user activity data be leveraged to improve the robustness and accuracy of AI/ML-based smart home security systems?

g) What mechanisms can be developed for enhance explainability, interpretability, and performance matrix in AI/ML models for real-time smart home security applications?

6. Results and Findings

The systematic review of literature from 2014 to 2025 encompassed 56 most relevant sources from different authentic sources from the domain of smart home IoT systems, security, privacy, and AI & ML–based attack detection and classifications. The review highlights a progressive evolution of smart home research, which is reflecting the transition from basic automation concepts to intelligent and smart, AI- and ML-driven intrusion detection systems.

Temporal Distribution of Publications: The publication trend indicates a sharp rise in research output post-2018, demonstrating the rapid expansion of interest in IoT-based smart home security and privacy.

Early years (2014–2017): Foundational research works focused on IoT architecture, connectivity protocols like Bluetooth, Zigbee, Wi-Fi, Z-Wave, 6LowPAN, and communication frameworks for smart homes and smart devices.

Mid years (2018–2021): Researches began to focusing on applications of AI and machine learning applications to enhancing technologies for anomaly detection, secure communication, and intrusion detection systems for data security and privacy in smart home environment. **Recent years (2022–2025):** Studies recent years focusing on integration of federated learning, blockchain, hybrid deep learning architectures (CNN, BiLSTM), and AI-based privacy protection was observed, signifying the convergence of AI and cybersecurity in smart environments.

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

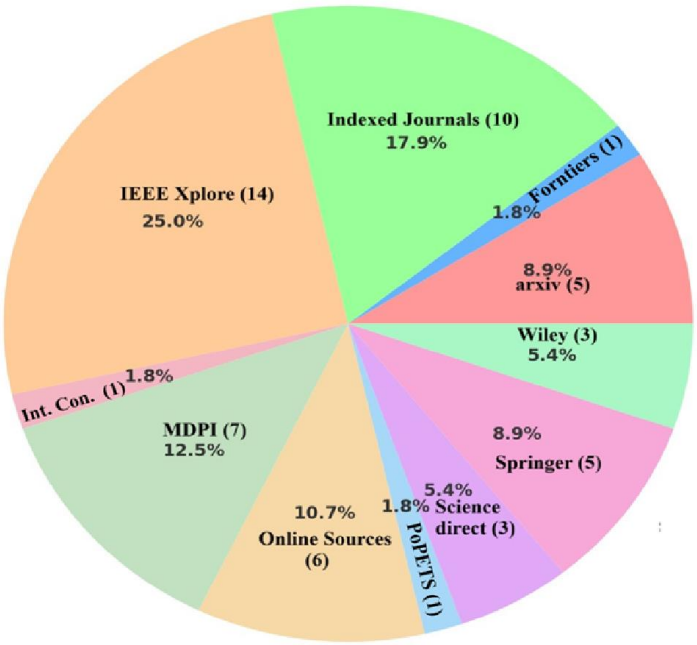


Figure 4: Source distribution

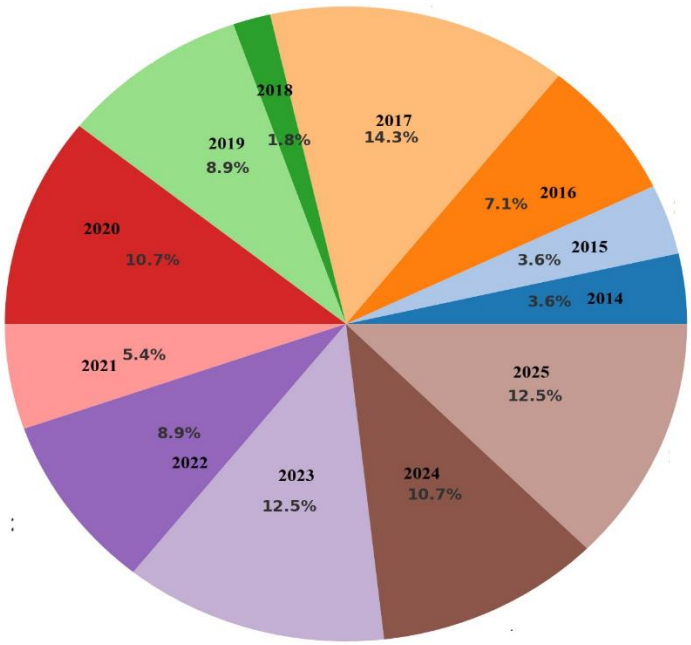


Figure 5: Year-wise papers distribution

Publication Source Analysis: More than 88% of sources of publications were referred form IEEE Xplore, MDPI, Wiley, Springer, indexed journals etc. This trend indicates that research in area of smart home security and privacy predominantly technology-based, supported by the computing and engineering sectors. A significant number of manuscripts pertaining to ML-based IDS and IoT privacy were presented at IEEE Access, IoT Journal, and Smart Cloud Conferences. Elsevier's Internet of Things Journal published comprehensive details on the multiple-communication protocols and their vulnerabilities, whereas MDPI's Sensors and Energies journals significantly advanced the studies on integrating IoT, ML, and cybersecurity.

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
Recent publications by Springer and Wiley Online Library dealt with federated learning and blockchain-based privacy-preserving smart home frameworks.

a) Thematic Analysis: The reviewed papers were categorized into the following dominant research themes:

Table -3: Thematic Analysis and key findings

S.no	Theme	Representative Studies	Key Findings and limitations
1	Smart Home IoT Architecture	[1], [3], [5], [9], [23]	Established the foundation of IoT layers (Perception, Communication, and Application) and their vulnerabilities. Limited only to architectural background study.
2	Communication Protocols & Vulnerabilities	From [10] to [22]	Identified protocol-specific attacks like DoS, bot attacks , replay, spoofing, man-in-the-middle etc. in Bluetooth, Wi-Fi, ZigBee, etc.
3	Intrusion Detection & Anomaly Detection	From [29] to [36], and from [45] to [49]	ML-based IDS (Decision Tree, RF, ANN, CNN, and LSTM) achieved accuracies between 95–99%. Most of studies are focus on attack detection and not utilize participatory approach of multiple models.
4	AI, Federated & Blockchain Models	From [42] to [44] and [51] to [56]	Introduced decentralized and privacy-aware learning systems improving detection accuracy and transparency. Need huge computational power, facing latency due to distributed architecture and data sharing issues.

b) Quantitative Findings: Machine Learning Superiority: Models such as Decision Tree, Random Forest, ANN, and RNN [45] [46][47] demonstrated impressive classification accuracy with more than 90+% in all ML based attack detection system in IoT environment and security systems.

c) Datasets Being Used: A growing focus on federated and edge computing is observed with the ACI-IoT, IEEEData Port, BoTIoT, UT-HAR, and CASAS datasets.
d) New Horizons: The 2023–2025 study agenda centers on lightweight IDS for edge IoT, ensemble learning, and hybrid federated learning and blockchain integration to the security systems but these systems has majorly computation power need , latency and data ownership issues.

e) **Trends and Insights:** There is a Strong shift from centralized ML models to the decentralized Federated Learning (FL) systems is observed. Along with the Integrity and trust were assured through blockchain technology for models. Studies also shows the adoption of the Explainable AI methodology, which were emphasizing on model transparency and interpretability, notably in home security. The Research paper repositories like IEEE, arXiv, MDPI, Springer etc have considerably enhanced the spread and reproducibility of research in IoT security.

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

f) Summary of Findings: Smart home systems are rapidly transforming into intelligent, adaptive, and secure ecosystems. The integration of AI, ML, and FL has significantly improved intrusion detection accuracy, though privacy and computational efficiency remain challenges. IEEE and Springer journals are leading contributors to this domain, reinforcing the credibility and technical orientation of ongoing research.

I have selected 56 research papers/article (most relevant to my area) out of more than 100+ research papers/articles from different authentic sources like IEEE, MDPI, Springer journal and other online sources related to smart home, smart home architecture, AI& ML based security models used in smart home's different areas as given in figure -4, and the paper selection criteria and its justification has discussed in table-4 as given below.

Table 4: Paper selection criteria form difference sources

S.no.	Criteria for selection of paper	Justification of criteria
1	The paper should be an original research paper and from authentic source	The original research paper from peer-reviewed indexed journals, authentic sources ensures scientific validity and academic integrity.
2	The suggested study should focus on Smart home communication protocols , machine learning techniques to find the security and privacy gap and can be applicable in smart home environments	The study seeks to analyses communication protocols security and privacy issues and incremental machine learning based IDS in IoT. So, papers/articles included in the study must have focus on different communication protocols, incremental ML approach to find out security and privacy issues in Smart home environment.
3	Only English language paper/article /source taken in consideration.	English language is very common and used by most of the authors.
4	The Smart home architecture, security model proposed/under study must be evaluated, analyzed by processing a real world dataset.	The study must be aimed to educate readers about the practicality of the suggested solutions, a goal that can be achieved through a thorough evaluation of these solutions.
5	The study must be published from 2014 to 2025 and study must be full length paper/article	The period of literature review is from 2014 to 2025. Full length paper contains the complete details
6	The paper/article must published in a peer reviewed journal /journals of repute or conference proceeding or the content form some authentic websites.	Journal articles/conference proceeding / authentic websites provide rigorously reviewed content.

IoT enabled networks are still having lots of security and privacy issues and challenges due to communication protocol issues, data encryption issue under the transmission due to low processing capability of sensor nodes and local storage when using local server to improve time sensitive data processing and need more improvements. So many research questions arise related to privacy and security of smart home data and network. Following are the research questions will consider for further improvement in smart home systems

Received: August 01, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
a) Can smart home system use tiny encryption algorithms or some variant of TES or some improved AES to enhance data security?

b) Can smart home contain some AI based approach to observe the smart home environment and data to analyze the different security and privacy threat and take corrective decision?

c) Can AI/ML based intrusion detection system use to observe the frequent connections of nodes and scan the metadata of transmitted packets to find out the abnormal/unwanted communication?

d) Can an efficient AI/ML/FD based cyber-attack identification, classification and mitigation system develop and integrate with smart home system for attack detection and attack response plan selection and execution, to minimize the attack loss.

7. Discussion

The evolution of smart home systems from simple automation to intelligent, connected ecosystems has transformed modern living with support of modern communication protocols like Bluetooth, WiFi, Zigbee, Zwave etc. However, the review of existing literature highlights significant gaps in terms of adaptive security, data privacy, and real-time decision-making. Although the use of Artificial Intelligence (AI) and Machine Learning (ML) models such as Logistic regression, ANN, Random Forest, CNN, and BiLSTM has enhanced intrusion detection and anomaly classification accuracy, most approaches remain limited by computational overhead, lack of expandability and heterogeneity of attack types. Recent studies report detection accuracies exceeding 99.9%, precision and recall values near 99%, and F1-scores beyond 98%, indicating strong model performance across multiple datasets for attack detection. Despite of such good metrics, the challenge lies in deployment of these models efficiently within resource-constrained smart home environments.
New developments like Federated Learning (FL) and Blockchain-supported model aggregation [44][52][53][54] deliver decentralized models for privacy-preserving and attack identification . Explainable AI (XAI) offers a gateway to understanding device behavior and rationalizing why people perform certain actions as suspicious. Increased transparency along with classification confidence with XAI-supported ANN frameworks is seen in studies like Sohail et al. [46]. The class of hybrid deep learning models which consists of BiLSTM–CNN and RNN-based frameworks is particularly robust in dealing with multi-protocol data (Zigbee, MQTT, LoRaWAN, Wi-Fi). However, embedding such models in heterogeneous IoT environments is still a work in progress. The present focus is on privacy-preserving, explainable, and distributed AI systems with autonomous threat detection, behavior analysis, and real-time mitigation capabilities in smart home networks.

8. Conclusion and future work

Smart home is collection of connected smart home appliances and it contains a well-defined architecture of nodes, central server and having the integration of edge and cloud processing. The appliances are connected through major communication protocols using majorly star or

Received: August 01, 2025

Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
mess topology but security and privacy in smart home environment is paramount and can't be compromised at any cost. The researches under review, state that, in spite of the vulnerabilities of smart homes with regard to privacy, security, and cyber threats, IoT based smart home solutions do provide comfort, efficiency, and safety. Lack of integration with diverse nature of devices, and security issues with protocols contribute to cyber threats. The success of Machine Learning Intrusion Detection Systems is unparalleled, with claim achievements of 99.9% accuracy and over 98% precision and recall with regard to attack detection, and claim explainability is improving to win user trust. Nevertheless, environment deployment remains challenging in terms of computation, latency, and privacy.

Utilizing the XAI frameworks offers a valuable avenue to address the current gaps of transparency and accountability in ML-based systems with computational overheads. The integration of federated learning, block chain technology, and lightweight AI will provide the foundation to build smart homes that are cyber-safe, scalable, and self-sufficient in detecting, classifying, and real-time neutralizing cyber threats, all while being privacy preserving. This study found following future work where researcher should focus to make smart home security and privacy more capable in terms of attack identification, classification and mitigation.

a) **Attack detection on basis of communication protocols metadata and resource utilization:** Experimenting and design an integrated framework with supervised, unsupervised and deep learning for more optimized accuracy matrices and multi-classification for modern attacks in smart home or IoT environment.
b) **Communication Protocol Security Frameworks:** Design frameworks to analyze protocol specific or heterogeneous traffic (MQTT, CoAP, Zigbee, LoRaWAN, WI-Fi) using hybrid ML models, for anomaly detection and attack multi-classification.
c) **Lightweight and Explainable AI Models:** Develop TinyML-based Explainable AI systems capable of real-time intrusion detection with reduced computational power while maintaining high accuracy and transparency.
d) **Federated and Blockchain Integration:** Combine Federated Learning with Blockchain to ensure decentralized model training, provenance verification, and tamper-proof data sharing among smart devices.
e) **Benchmarking and Dataset Expansion:** Establish large-scale, labeled smart home datasets integrating behavioral and network data (e.g., FRIoT, CADeSH) to train and evaluate explainable AI-based IDS models.
f) **Energy-Aware and Sustainable IDS Systems:** Develop power-efficient AI models optimized for continuous monitoring without compromising accuracy or latency.

Future research should move toward self-learning, interpretable, and privacy-enhanced AI-driven security architectures that balance detection accuracy, computational efficiency, and human trust for next-generation smart homes.

References

1. "Smart Home – India " URL:https://www.statista.com/outlook/dmo/smart-home/india year : 2021 last seen Feb -2022

Received: August 01, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
2. Saber Talari , Miadreza Shafie-khah , Pierluigi Siano , Vincenzo Loia "A Review of Smart Cities Based on the Internet of Things Concept" Energies 2017, 10, 421; oi:10.3390/en10040421 available at http://www.mdpi.com/journal/energies
3. Rakesh Roshan and Abhay Kr. Ray "Challenges and Risk to Implement IOT in Smart Homes: An Indian Perspective" International Journal of Computer Applications (0975 – 8887) Volume 153 – No3, November 2016
4. Menal Dahiya ," Issues and Countermeasures for Smart Home Security" e-ISSN: 2394 – 3343 p-ISSN: 2394 – 5494 International Journal of Innovative and Emerging Research in Engineering Volume 4, Issue 5, 2017.
5. Pallavi Sethi and Smruti R. Sarangi "Internet of Things: Architectures, Protocols, and Applications" Journal of Electrical and Computer Engineering Volume 2017, Article ID 9324035, 25 pages https://doi.org/10.1155/2017/9324035
6. Saber Talari , Miadreza Shafie-khah , Pierluigi Siano , Vincenzo Loia "A Review of Smart Cities Based on the Internet of Things Concept" Energies year :2017, 10, 421; Doi:10.3390/en10040421 available at http://www.mdpi.com/journal/energies
7. Rakesh Roshan and Abhay Kr. Ray " Issues, challenges and application of big data in smart home " International Journal of Computer Applications (0975 – 8887) International Conference on "Computer Systems & Mathematical Sciences" (ICCSMS 2016) URL : https://research.ijcaonline.org/iccsms2016/number1/iccsms201665.pdf year 2016
8. Drew Hendricks "The History of Smart Homes", published on April 22, 2014 URL : https://www.iotevolutionworld.com/m2m/articles/376816-history-smart-homes.htm last seen : Dec -2021
9. John A Sankovic, Life Fellow IEEE "Research Directions for the Internet of Things " 2014 IEEE url : https://ieeexplore.ieee.org/document/6774858
10. P. Cope, J. Campbell and T. Hayajneh, "An investigation of Bluetooth security vulnerabilities," Year: 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), 2017, pp. 1-7, doi: 10.1109/CCWC.2017.7868416.
11. Kalinin, E.; Belyakov, D.; Bragin, D.; Konev, A. IoT Security Mechanisms in the Example of BLE. *Computers* 2021, *10*, 162. https://doi.org/10.3390/computers10120162
12. Alireza Zohourian, Sajjad Dadkhah, et al. "IoT Zigbee device security: A comprehensive review, Internet of Things" Volume 22, 2023, 100791, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2023.100791. URL: https://www.sciencedirect.com/science/article/pii/S2542660523001142
13. Kyounggon Kim, Kiyoon Cho et al. "What's your protocol: Vulnerabilities and security threats related to Z-Wave protocol, Pervasive and Mobile Computing" Volume 66, 2020, 101211, ISSN 1574-1192, https://doi.org/10.1016/j.pmcj.2020.101211. URL : https://www.sciencedirect.com/science/article/pii/S1574119220300742

Received: August 01, 2025

Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
14. N. b. H. Kasah, A. H. b. M. Aman, Z. S. M. Attarbashi and Y. Fazea, "Investigation on 6LoWPAN Data Security for Internet of Things," *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, Sakaka, Saudi Arabia, 2020, pp. 1-5, doi: 10.1109/ICCIS49240.2020.9257661.
15. A. Halbouni, L. -Y. Ong and M. -C. Leow, "Wireless Security Protocols WPA3: A Systematic Literature Review," in IEEE Access, vol. 11, pp. 112438-112450, 2023, doi: 10.1109/ACCESS.2023.3322931.
16. Savadatti, Shreya, KuldeepDhariwal, Sakshi, Krishnamoorthy, Shruthi, Delhibabu, Radhakrishnan, An Extensive Classification of 5G Network Jamming Attacks, Security and Communication Networks, 2024, 2883082, 23 pages, 2024. https://doi.org/10.1155/2024/2883082
17. Lucian Armas "Thread Protocol: Enabling Secure Mesh Networks For Smart Home Devices" URL :http://www.tomshardware.com/news/thread-mesh-networking-protocol-homes,29556.html year 2015 last seen Dec 2024
18. Clemens Valens "LoRaWAN security vulnerabilities Exposed" Oct 2016 last seen Dec 2024 URL : https://www.elektormagazine.com/news/lorawan
19. Onumadu, P.; Abroshan, H. near-Field Communication (NFC) Cyber Threats and Mitigation Solutions in Payment Transactions: A Review. Sensors 2024, 24, 7423. https://doi.org/10.3390/s24237423
20. "Make things come alive in a secure way- Sigfox" Feb 2017 last seen Dec 2024 URL : https://www.sigfox.com/sites/default/files/1701-SIGFOX-White_Paper_Security.pdf
21. S. Arvind and V. A. Narayanan, "An Overview of Security in CoAP: Attack and Analysis," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), 2019, pp. 655-660, doi: 10.1109/ICACCS.2019.8728533.
22. F. Chen, Y. Huo, J. Zhu and D. Fan, "A Review on the Study on MQTT Security Challenge," 2020 IEEE International Conference on Smart Cloud (SmartCloud), 2020, pp. 128-133, doi: 10.1109/SmartCloud49737.2020.00032.
23. Belli, D., Barsocchi, P., & Palumbo, F. (2024). Connectivity Standards Alliance Matter: State of the art and opportunities. Internet of Things, 25, 101005.
24. Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-FovinoGary Steri, and Gianmarco Baldini "Security and Privacy Issues for an IoT based Smart Home" MIPRO 2017, May 22- 26, 2017, Opatija, Croatia
25. Aimin Yang, Chunying Zhang, Yongjie Chen, Yunxi Zhuansun, Huixiang Liu " Security and Privacy of Smart Home Systems Based on the Internet of Things and Stereo Matching Algorithms " IEEE the Internet of Things 2327-4662 (c) 2019 IEEE.
26. Khushal Shingala, Jignesh Patel "Automatic Home Appliances and Security of Smart Home with RFID,SMS, Email and Real Time Algorithm Based on IOT"International Research Journal of Engineering and Technology (IRJET) Volume: 04 Issue: 04 Apr -2017 e-ISSN: 2395 -0056 p-ISSN: 2395-0072

Received: August 01, 2025

Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
27. Vaishnavi S. Gunge ,Pratibha S. Yalagi "Smart Home Automation: A Literature Review" International Journal of Computer Applications (0975 – 8887) year 2016
28. J. Bugeja, A. Jacobsson and P. Davidsson, "A Privacy-Centered System Model for Smart Connected Homes," 2020 IEEE International Conference on Pervasive Computing and Communications Workshops, 2020, pp.1-4, doi: 10.1109/ PerComWorkshops 48775.2020.9156246.
29. Supriya Nagarkar, Dr.Vikas Prasad " Evaluating Privacy and Security Threats in IoT based Smart Home Environment " International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 7, 2019 (Special Issue) Research India Publications. http://www.ripublication.com
30. F. Liang, W. G. Hatcher, W. Liao, W. Gao, and W. Yu, ‘‘Machine learning for security and the Internet of Things: The good, the bad, and the ugly,’’ IEEE Access, vol. 7, pp. 158126–158147, 2019
31. E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," in *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042-9053, Oct. 2019, doi: 10.1109/JIOT.2019.2926365.
32. Cui, L., Yang, S., Chen, F. et al. A survey on application of machine learning for Internet of Things. Int. J. Mach. Learn. & Cyber. 9, 1399–1417 (2018). https://doi.org/10.1007/s13042-018-0834-5
33. S. Ramapatruni, S. N. Narayanan, S. Mittal, A. Joshi and K. Joshi, "Anomaly Detection Models for Smart Home Security," 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, DC, USA, 2019, pp. 19-24, doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00015.
34. F. Alghayadh and D. Debnath, "HID-SMART: Hybrid Intrusion Detection Model for Smart Home," 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2020, pp. 0384-0389, doi: 10.1109/CCWC47524.2020.9031177.
35. N. Elsayed, Z. S. Zaghloul, S. W. Azumah and C. Li, "Intrusion Detection System in Smart Home Network Using Bidirectional LSTM and Convolutional Neural Networks Hybrid Model," 2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS), Lansing, MI, USA, 2021, pp. 55-58, doi: 10.1109/MWSCAS47672.2021.9531683.
36. E. D. Alalade, "Intrusion Detection System in Smart Home Network Using Artificial Immune System and Extreme Learning Machine Hybrid Approach," 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2020, pp. 1-2, doi: 10.1109/WF-IoT48130.2020.9221151.
37. Y. Meidan, D. Avraham, H. Libhaber and A. Shabtai, "CADeSH: Collaborative Anomaly Detection for Smart Homes," arXiv: 2303.01021, Mar. 2023. [Online]. Available: https://arxiv.org/abs/2303.01021.

Received: August 01, 2025

38. Y. Majib, M. Alosaimi, A. Asaturyan and C. Perera, "Dataset for cyber–physical anomaly detection in smart homes," Frontiers in the Internet of Things, vol. 2, Art. 1275080, Oct. 2023, doi: 10.3389/friot.2023.1275080.

39. S. Manandhar, K. Kafle, B. Andow, K. Singh and A. Nadkarni, "Smart Home Privacy Policies Demystified," in Proc. 31st USENIX Security Symposium, 2022. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/manandhar.

40. I. Zavalyshyn, A. Legay, A. Rath and E. Rivière, "SoK: Privacy-enhancing Smart Home Hubs," Proc. PoPETs, 2022. [Online]. Available: https://petsymposium.org/popets/2022/popets-2022-0097.pdf.

41. Xuan Dai, Jian Mao, Jiawei Li,Qixiao Lin, and Jianwei Liu , "HomeGuardian: Detecting Anomaly Events in Smart Home Systems," 2022. [Online]. url: https://onlinelibrary.wiley.com/doi/10.1155/2022/8022033

42. Ayan . Chatterjee, "IoT anomaly detection methods and applications: A survey," 2022. [Online] url : https://arxiv.org/pdf/2207.09092

43. Samiul Alam ,Tuo Zhang,Tiantian Feng et al. "FedAIoT: A Federated Learning Benchmark for AIoT," arXiv: 2310.00109, Oct. 2023. [Online]. Available: https://arxiv.org/abs/2310.00109; GitHub: https://github.com/AIoT-MLSys-Lab/FedAIoT.

44. Y. Zhang et al., "Privacy-Aware Anomaly Detection in IoT Environments (FedGroup)," J. Netw. Comput. Appl., 2023. doi: 10.1007/s10922-023-09782-9. URL: https://link.springer.com/article/10.1007/s10922-023-09782-9

45. Sujit Biswas, "Blockchain controlled trustworthy federated learning platform for smart homes," Open repository, 2024. [Online]. URL : https://ietresearch.onlinelibrary.wiley.com/doi/epdf/10.1049/cmu2.12870 DOI:10.1049/cmu2.12870

46. S. M. Vanen et al. "An Improved Intrusion Detection Scheme in a Smart Home Environment," International Journal of Computer Applications volume- 186, Number 74, page No. 42–53, March 2025, doi: 10.5120/ijca2025924607.

47. Shaleeza Sohail, Zongwen Fan et al “Explainable and optimally configured artificial neural networks for attack detection in smart homes” May-2022. https://doi.org/10.48550/arXiv.2205.08043 url: https://arxiv.org/abs/2205.08043

48. Aljabri, M., Shaahid, A., Alnasser, F., Saleh, A., Alomari, D., Aboulnour, M., Althubaity, A. (2024). "IoT Attacks Detection Using Supervised Machine Learning Techniques” HighTech and Innovation Journal, 5(3), 534–550. https://doi.org/10.28991/HIJ-2024-05-03-01

49. Ali H. Farea, and Kerem Kucuk , "Machine Learning-based Intrusion Detection Technique for IoT: Simulation with Cooja ", International Journal of Computer Network and Information Security (IJCNIS), Vol.16, No.1, pp.1-23 2024. DOI:10.5815/ijcnis.2024.01.01

50. Aldaej, A., Ahanger, T.A, Ullah, I. "Deep Learning-Inspired IoT-IDS Mechanism for Edge Computing Environments”. Sensors 2023, 23, 9869. https://doi.org/10.3390/s23249869

Received: August 01, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
51. M. Shalan, M. R. Hasan, Y. Bai, and J. Li, "Enhancing Smart Home Security: Blockchain-Enabled Federated Learning with Knowledge Distillation for Intrusion Detection," *Smart Cities*, vol. 8, no. 1, Art. 035, Feb. 2025, doi: 10.3390/smartcities8010035.

52. Ansam Khraisat, Ammar Alazab et al. "Federated Learning for Intrusion Detection in IoT Environments: A Privacy-Preserving Strategy," *Discover Internet of Things*, vol. 5, Art. 072, Jun. 2025, doi: 10.1007/s43926-025-00169-7.

53. S. B. Wankhede and D. Patel, "Federated Learning and Blockchain Approach for Securing IoT Data," *Discover Internet of Things*, vol. 5, Art. 116, Oct. 2025, doi: 10.1007/s43926-025-00234-1.

54. A. Deshmukh, P. E. de la Rosa, R. V. Rodriguez, and S. Dasari, "Enhancing Privacy in IoT-Enabled Digital Infrastructure: Evaluating Federated Learning for Intrusion and Fraud Detection," *Sensors*, vol. 25, no. 10, Art. 3043, May 2025, doi: 10.3390/s25103043.

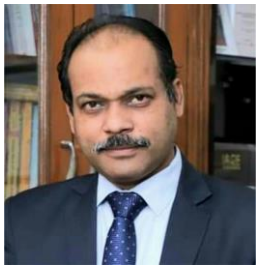
55. Atul Kumar, Bhisham Sharma & Ajit Noonia "Secure Blockchain Based Intrusion Detection for IoT Networks," *Discover Computing*, vol. 28, Art. 226, Oct. 2025, doi: 10.1007/s10791-025-09754-4.

56. M. Rahmati et al. "Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy-Preserving and Real-Time Threat Detection Capabilities," *arXiv*, Feb. 2025.

Authors Bio:

	Abhay Kumar Ray is research scholar in Department of Computer applications, SRM- Institute of Science & Technology, Delhi –NCR Campus, Modinagar, Ghaziabad. He holds degrees of MCA (Master of computer Applications). He has published several papers in national and international journals and conferences and conducted 50+ workshop on cutting edge technologies in different institutes of India. Mr. Ray has experience of 16 years in both industry and academia, his area of interest is Internet of Things (IoT), Web Programming, Security System and Artificial Intelligence and Machine Learning.
	Dr. Rupak Sharma is an Associate Professor and Head of the Department of Computer Applications at SRM Institute of Science & Technology (SRMIST), Delhi-NCR Campus. He completed his PhD in Computer

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	Science & Engineering from Singhania University (Rajasthan) in 2012 and holds an MCA from Meerut Institute of Engineering & Technology. His research interests include artificial intelligence, machine learning, IoT, cloud computing, and mobile / ad-hoc networks. Dr. Sharma has published numerous peer-reviewed conference and journal papers, including in IEEE and Elsevier venues. Some of his recent works include AI-driven systems for physiological forecasting, IoT-based monitoring of industrial machines, and robotics for disinfection applications. He is passionate about mentoring students in emerging areas of computing and has guided both undergraduate and postgraduate research projects.
	Dr. Sunil Kumar Pandey is currently working as Professor in Institute of Technology & Science with an experience of over 24+ Years in Industry and Academia and having interest in Cloud, Blockchain, Database Technologies & Soft Computing. He has been credited with 65+ Research papers (including SCI/ Scopus Indexed), 03 Book Chapters and 3 Books with reputed publishers including Springer, IGI, IEEE Xplore, River Press – Denmark, Wiley, Hindawi, Journals/ Conferences. He has been a regular author of Articles in different Print and Online Platforms including Interviews, Views and has published 11 edited volumes on different relevant themes of Information Technologies. He has been providing & coordinating training and consultancy to various reputed organizations including Indian Air Force and has conducted 25+ National/ International Conferences/ Summits/ Conclaves in association with AICTE, CSI, DST and other leading organizations. He has also conducted large number of FDP/Entrepreneurship Programs supported by AICTE/ DST/ UGC/ EDI etc.

Received: August 01, 2025