

VOLUME 1

|

NUMBER 1

|

JUNE 2026

JOURNAL OF

SECURE DIGITAL TECHNOLOGIES

A PEER-REVIEWED JOURNAL

BRIDGING TECHNOLOGY, LAW AND TRUST

IN THE DIGITAL AGE

DGSC, Astana, Kazakhstan

Journal of Secure Digital Technologies

Volume 1 (№1) June 2026

Sertificate № KZ19VPY00128988, date of issue: 25.12.2025

*The journal is published 4 times a year
(March, June, September, December)*

EDITORIAL TEAM

Editor-in-Chief

Dr. Leila Rzayeva, Association prof., PhD, Digital government support center (Kazakhstan)

Deputy Editor-in-Chief

Dr. Ali Myrzatay, PhD, Digital government support center (Kazakhstan)

Executive Secretary

Dr. Abdenova Zhuldyz, PhD, Digital government support center (Kazakhstan)

EDITORIAL BOARD MEMBERS (KAZAKHSTAN)

Seitkulov E.N. – Candidate of Physical and Mathematical Sciences, Professor Computer Science, Computer Engineering and Control

Abdenova G.A. – PhD in Automation and Control, Candidate of Technical Sciences, Professor L.N. Gumilyov Eurasian National University

Atanov S.K. – Doctor of Technical Sciences, Professor.

Sergazin G.K. – PhD, Associate Professor Computer Science, Computer Engineering and Control

Satybaldina D.Zh. – Candidate of Physical and Mathematical Sciences, Professor Director, Research Institute of Information Security and Cryptology, L.N. Gumilyov Eurasian National University

INTERNATIONAL EDITORIAL BOARD MEMBERS

Ibraheem Shayea – PhD in Electrical and Electronic Engineering Istanbul Technical University (Turkey)

Yadigar Nasiboglu Imamverdiyev – DSc in Technical Sciences, Associate Professor Information Security, Computer Science and Computer Technology (Azerbaijan)

Erdal Irmak – PhD in Electrical and Electronics Engineering, Professor Gazi University (Turkey)

Korhan Kayisli – PhD in Electrical Electronics Engineering, Associate Professor Gazi University (Turkey)

Yonghao Wang – PhD in Electronic Engineering, Associate Professor Queen Mary, University of London (UK)

Amir Mosavi – PhD in Applied Informatics, Professor of AI Obuda University (Hungary)

Gerald Feldman – PhD in General Computing, Associate Professor Birmingham City University (UK)

Mohamed Ragab – PhD in Computer Science, Assistant Professor Birmingham City University (UK)

Seref Sagiroglu – PhD in System Engineering, Professor Gazi University (Turkey)

MANAGING EDITOR

Dr. Ali Myrzatay, PhD, Digital government support center (Kazakhstan)

TECHNICAL EDITOR

Dr. Ali Myrzatay, PhD, Digital government support center (Kazakhstan)

CONTENTS

A Multi-Level Strategy for IT Risk Management with LLM-Based Risk Identification.....	3
Securing the Physical-Digital Frontier: AI for Anomaly Detection in OT, IoT, and Critical Infrastructure.....	22
Forensic Transcription of Kazakh Speech Evidence: Evaluating Whisper and LLM Post-Correction Reliability.....	34
Legal Admissibility of Machine Learning Reconstructed Data in Digital Forensics	51
The Cybersecurity Risks of Generative AI: Attack and Defense Perspectives.....	66
Smart Home Vulnerabilities: Studying the Security Risks and Unauthorized Access Considerations Inherent to Everyday IoT Devices.....	78
Machine Learning for Network Intrusion Detection Under Class Imbalance and Feature Pruning.....	92

Temirlan Zhaxalykov

MSc, Senior Lecturer, School of Information Technology and Engineering, Kazah-British Technical University
t.zhaxalykov@kbtu.kz, 0000-0002-6994-6377
Kazakh-British Technical University, Kazakhstan

Olzhas Myrzabek

Student, Software Engineering, Astana IT University, Kazakhstan
olzhas.myrzabek@astanait.edu.kz
Astana IT University, Kazakhstan

Sanida Yessenbek

Senior lecturer, Supervisor, Astana IT University, Kazakhstan
Astana IT University, Kazakhstan

SMART HOME VULNERABILITIES: STUDYING THE SECURITY RISKS AND UNAUTHORIZED ACCESS CONSIDERATIONS INHERENT TO EVERYDAY IoT DEVICES

Abstract: Background: Smart home ecosystems integrate Internet of Things (IoT) devices—cameras, door locks, voice assistants, thermostats, and lighting controllers—into residential networks that process sensitive personal data and control physical access. As adoption accelerates, these devices introduce attack surfaces that differ fundamentally from traditional enterprise IT systems. Objective: This study systematically examines security risks and unauthorized access vectors affecting consumer-grade smart home IoT devices. Methods: A mixed-methods security assessment was conducted on twelve commercially available devices from four manufacturers. The methodology combined passive network traffic analysis, firmware inspection, automated vulnerability scanning with Nmap and OpenVAS, manual penetration testing guided by the OWASP IoT Top 10, and a structured review of 47 peer-reviewed publications published between 2020 and 2025. Results: Analysis identified 38 distinct vulnerabilities across the test corpus, including 14 critical and 11 high-severity findings. Default or weak credentials were present on 67 % of devices; 58 % transmitted credentials or tokens over unencrypted channels during initial pairing; 42 % exposed administrative interfaces on the local network without authentication. Unauthorized access was demonstrated on five devices through credential replay, firmware downgrade, or cloud API token extraction. Conclusions: Consumer smart home deployments exhibit systemic weaknesses in authentication, update mechanisms, and network segmentation. The study contributes a reproducible assessment framework and evidence-based mitigation recommendations for homeowners, manufacturers, and policymakers seeking to reduce unauthorized access in residential IoT environments.

Keywords: *smart home security; Internet of Things; unauthorized access; vulnerability assessment; consumer IoT; network security; firmware analysis; penetration testing*

Уязвимости Умного Дома: Исследование Рисков Безопасности и Проблем Несанкционированного Доступа, Присущих Повседневным IoT-Устройствам

Аннотация: Введение. Экосистемы умного дома объединяют устройства Интернета вещей (IoT) — камеры, дверные замки, голосовые помощники, термостаты и контроллеры освещения — в домашние сети, обрабатывающие конфиденциальные персональные данные и управляющие физическим доступом. По мере ускорения внедрения такие устройства создают поверхности атаки, принципиально отличающиеся от традиционных корпоративных ИТ-систем. Цель. Данное исследование систематически анализирует риски безопасности и векторы несанкционированного доступа, затрагивающие потребительские IoT-устройства умного дома. Методы. Проведена комплексная оценка безопасности двенадцати коммерчески доступных устройств от четырёх производителей. Методология сочетала пассивный анализ сетевого трафика, инспекцию прошивки, автоматическое сканирование уязвимостей с помощью Nmap и OpenVAS, ручное тестирование на проникновение по методике OWASP IoT Top 10, а также структурированный обзор 47 рецензируемых публикаций, вышедших в 2020–2025 годах. Результаты. Анализ выявил 38 отдельных уязвимостей во всём тестовом корпусе, включая 14 критических и 11 находок высокой степени серьёзности. Стандартные или слабые учётные данные присутствовали на 67 % устройств; 58 % передавали учётные данные или токены по незашифрованным каналам при первоначальном сопряжении; 42 % открывали административные интерфейсы в локальной сети без аутентификации. Несанкционированный доступ был продемонстрирован на пяти устройствах посредством повторного использования учётных данных, отката прошивки или извлечения токена облачного API. Заключение. Потребительские развёртывания умного дома демонстрируют системные слабости в аутентификации, механизмах обновления и сегментации сети. Исследование вносит вклад в виде воспроизводимой системы оценки и рекомендаций по снижению рисков, основанных на фактических данных, для домовладельцев, производителей и регуляторов, стремящихся снизить несанкционированный доступ в жилых IoT-средах.

Ключевые слова: безопасность умного дома; Интернет вещей; несанкционированный доступ; оценка уязвимостей; потребительский IoT; сетевая безопасность; анализ прошивки; тестирование на проникновение

Ақылды Үй Осалдықтары: Күнделікті IoT Құрылғыларына Тән Қауіпсіздік Тәуекелдері мен Рұқсатсыз Қол Жеткізу Мәселелерін Зерттеу

Андатпа: Кіріспе. Ақылды үй экожүйелері Интернет заттары (IoT) құрылғыларын — камералар, есік құлыптары, дауыстық көмекшілер, термостаттар және жарықтандыру контроллерлерін — құпия жеке деректерді өңдейтін және

физикалық қол жеткізуді басқаратын тұрғын үй желілеріне біріктіреді. Енгізу қарқыны артқан сайын, бұл құрылғылар дәстүрлі корпоративтік IT жүйелерінен түбегейлі ерекшеленетін шабуыл беттерін тудырады. Мақсаты. Бұл зерттеу тұтынушылық ақылды үй IoT құрылғыларына әсер ететін қауіпсіздік тәуекелдері мен рұқсатсыз қол жеткізу векторларын жүйелі түрде зерттейді. Әдістер. Төрт өндірушінің он екі коммерциялық қолжетімді құрылғысына аралас әдістемелік қауіпсіздік бағалауы жүргізілді. Әдістеме желілік трафикті пассивті талдауды, микробағдарламаны тексеруді, Nmap және OpenVAS арқылы автоматтандырылған осалдықтарды сканерлеуді, OWASP IoT Top 10 бойынша қолмен енуді тестілеуді, сондай-ақ 2020–2025 жылдары жарияланған 47 рецензияланған басылымға құрылымдық шолуды біріктірді. Нәтижелер. Талдау тест корпусында 14 критикалық және 11 жоғары дәрежелі табылымды қоса алғанда, 38 бөлек осалдықты анықтады. Әдепкі немесе әлсіз тіркелгі деректері құрылғылардың 67 %-ында болды; 58 %-ы бастапқы жұптасу кезінде тіркелгі деректерін немесе токендерді шифрланбаған арналар арқылы жіберді; 42 %-ы аутентификациясыз жергілікті желіде әкімшілік интерфейстерді ашық қалдырды. Рұқсатсыз қол жеткізу бес құрылғыда тіркелгі деректерін қайта пайдалану, микробағдарламаны төмендету немесе бұлттық API токенін алу арқылы көрсетілді. Қорытынды. Тұтынушылық ақылды үй жүйелері аутентификацияда, жаңарту тетіктерінде және желіні сегменттеуде жүйелік әлсіздіктерді көрсетеді. Зерттеу тұрғын үй IoT ортасында рұқсатсыз қол жеткізуді азайтуға ұмтылатын үй иелері, өндірушілер және саясаткерлер үшін қайта жаңғыртылатын бағалау жүйесі мен дәлелдерге негізделген төмендету ұсыныстарын қамтамасыз етеді.

Түйін сөздер: *ақылды үй қауіпсіздігі; Интернет заттары; рұқсатсыз қол жеткізу; осалдықты бағалау; тұтынушылық IoT; желілік қауіпсіздік; микробағдарлама талдауы; енуді тестілеу*

1. Introduction (Literature Review)

Residential smart home technology has transitioned from a niche luxury to a mainstream consumer category. Industry analysts estimate that more than 1.8 billion IoT devices were deployed in homes worldwide by 2025, with annual shipment growth exceeding 12 % [1]. These devices automate lighting, climate control, surveillance, and physical access while continuously collecting behavioural and biometric data. Unlike enterprise systems protected by dedicated security teams, smart home deployments are typically configured by non-expert users on consumer-grade routers with minimal network segmentation [2]. Consequently, a compromised smart camera or door lock can serve as a pivot point for lateral movement within a home network or for unauthorized remote control of physical assets [3].

Literature Review. Research on IoT security has expanded rapidly over the past decade. Antwi and colleagues [4] conducted a systematic review of 112 studies and

identified authentication weaknesses, insufficient encryption, and insecure firmware update mechanisms as the three most frequently reported vulnerability classes in consumer IoT. Al-Garadi and co-authors [5] mapped attack vectors across the IoT architecture stack, demonstrating that vulnerabilities at the perception layer (sensors and actuators) propagate upward to application and cloud layers when devices share credentials or trust boundaries are poorly defined. Sivaraman and colleagues [6] showed that many smart home hubs fail to enforce mutual authentication between peripheral devices, enabling rogue device injection attacks on Zigbee and Z-Wave networks.

Penetration testing studies provide empirical evidence of exploitable weaknesses. Garcia-Teodoro et al. [7] evaluated 20 commercial IP cameras and found that 65 % permitted remote access with factory-default credentials or credentials recoverable from firmware images. Kolias et al. [8] demonstrated large-scale exploitation of IoT botnets such as Mirai and Mozi, in which compromised home devices were recruited into distributed denial-of-service networks within hours of internet exposure. More recent work by Neshenko et al. [9] highlights the growing threat of supply-chain compromises in IoT firmware, where malicious code is injected before devices reach consumers.

Regulatory and standardisation efforts have attempted to address these gaps. The European Union Cyber Resilience Act and the U.S. Cyber Trust Mark programme establish baseline security requirements for connected consumer devices [10]. The IoT Security Foundation's best-practice guidelines recommend unique device credentials, signed firmware updates, and disablement of unused services [11]. However, compliance remains voluntary in most jurisdictions, and independent testing reveals persistent gaps between vendor claims and observed security posture [12]. Studies focusing specifically on smart home ecosystems rather than generic IoT—such as those by Jacobsson and Boldt [13] and Alrawi et al. [14]—have shown that device interdependencies (e.g., a voice assistant controlling door locks) amplify the blast radius of a single compromise, yet holistic security assessments of multi-vendor home environments remain scarce.

Research Gap. Although individual device classes (cameras, hubs, voice assistants) have been studied in isolation, few studies provide a unified, reproducible methodology for assessing unauthorized access risk across heterogeneous smart home deployments representative of typical consumer configurations. Existing surveys synthesise published vulnerabilities but rarely validate findings through controlled hands-on testing of current-generation devices. Furthermore, the interaction between local network exposure, cloud API security, and mobile application credential storage is insufficiently characterised in the residential context.

Research Question(s). This study addresses the following research question: What security vulnerabilities and unauthorized access vectors are present in commonly deployed consumer smart home IoT devices, and how can they be systematically identified and mitigated? Specifically, the paper examines: (1) the prevalence and severity of authentication, encryption, and firmware-related weaknesses; (2) the feasibility of

unauthorized local and remote access through practical exploitation; and (3) the effectiveness of recommended countermeasures when applied to a representative home network topology.

Scientific Novelty. The scientific novelty of this work consists in the integration of a structured literature-derived threat taxonomy with a hands-on, multi-layer assessment protocol applied simultaneously to devices spanning video surveillance, access control, environmental control, and voice interaction categories. Unlike prior device-specific case studies, this approach evaluates cross-device attack paths —such as leveraging a compromised smart speaker to extract cloud tokens used by a door lock—which distinguishes it from prior approaches that treat each device category independently.

Contributions. The main contributions of this paper are:

A reproducible smart home IoT security assessment framework aligned with OWASP IoT Top 10 and NIST IR 8259 guidelines;

Empirical vulnerability data from twelve current-generation consumer devices, including severity ratings and exploit confirmation rates;

Demonstration of five practical unauthorized access scenarios with documented attack chains;

Evidence-based mitigation checklist for homeowners, device manufacturers, and regulatory bodies.

The remainder of the paper is organized as follows: Section 2 presents the materials and assessment methodology; Section 3 reports empirical findings; Section 4 discusses implications and answers the research questions; Section 5 concludes the paper.

2. Methods and Materials

This section describes the devices under test, the laboratory network topology, assessment tools, and the procedural steps followed to ensure reproducibility. All experiments were conducted in an isolated laboratory environment; no production or third-party networks were targeted.

2.1 Device Selection and Test Environment

Twelve consumer IoT devices were selected to represent four functional categories: video surveillance (3 devices), access control (3 devices), environmental control (3 devices), and voice assistants/hubs (3 devices). Selection criteria required devices to rank among the top 50 best-selling models on major e-commerce platforms in 2024–2025, support cloud connectivity, and be purchasable in the Republic of Kazakhstan. Devices were assigned anonymous identifiers D1–D12 to avoid vendor bias in reporting.

The test environment replicated a typical home network: a consumer Wi-Fi router (TP-Link Archer AX73), a /24 private subnet (192.168.1.0/24), and a dedicated VLAN (192.168.50.0/24) for IoT isolation experiments. A Kali Linux 2024.4 workstation and a Raspberry Pi 4 passive monitoring node were connected via Ethernet. Internet access was provided through a controlled gateway permitting packet capture.

2.2 Assessment Methodology

Assessment followed four phases over a nine-week period: (Phase 1) passive reconnaissance and traffic analysis using Wireshark 4.2 and Zeek 6.0; (Phase 2) active scanning with Nmap 7.94 and OpenVAS 22.7; (Phase 3) manual penetration testing guided by the OWASP IoT Top 10 (2024 edition) and MITRE ATT&CK for ICS/IoT techniques; (Phase 4) firmware extraction and static analysis using Binwalk 2.3 and Ghidra 11.0 where legally permitted by device design (developer mode or publicly available update images).

Each identified vulnerability was classified using the Common Vulnerability Scoring System (CVSS v3.1) and mapped to CWE identifiers. Unauthorized access attempts were documented with proof-of-concept procedures but were not weaponised beyond the laboratory scope. A structured literature review of 47 peer-reviewed sources (2020–2025) was conducted in parallel to contextualise empirical findings.

2.3 Ethical and Legal Considerations

All testing was performed on devices owned by the research team within an isolated laboratory. Responsible disclosure was initiated for critical findings prior to publication, in accordance with vendor vulnerability disclosure policies. No personal data from external users was collected or processed.

Table 1. Assessment phases and tooling.

Assessment Phase	Tools	Primary Output
Passive analysis	Wireshark, Zeek	Protocol inventory, cleartext credential detection
Active scanning	Nmap, OpenVAS	Open port/service map, CVE matches
Manual testing	Burp Suite, mitmproxy	Authentication bypass, API abuse
Firmware analysis	Binwalk, Ghidra	Hardcoded keys, unsigned update channels

2.4 Threat Model and Assessment Checklist

A threat model was constructed following STRIDE methodology adapted for residential IoT. Trust boundaries were defined at: (T1) the internet gateway, (T2) the home LAN, (T3) the IoT VLAN, (T4) device firmware, and (T5) cloud service endpoints. For each boundary, attacker capabilities were modelled at three levels: opportunistic (automated scanning), targeted (local network adversary), and advanced (nation-state or organised crime with supply-chain access). A 42-item assessment checklist was derived from NIST IR 8259

[16], OWASP IoT Top 10 [15], and ETSI EN 303 645, covering identity management, secure update, data protection, and resilience requirements.

Device categories and representative functions under test are summarised in Table 4. Voice assistants and hubs were included because they frequently act as aggregation points controlling multiple downstream devices, making them high-value targets for unauthorized access attempts.

Table 4. Device categories under assessment.

ID	Category	Primary Interface	Cloud Dependency
D1–D3	Video surveillance	Wi-Fi, RTSP	Yes
D4–D6	Access control	Wi-Fi, BLE, Zigbee	Partial
D7–D9	Environmental control	Wi-Fi, MQTT	Yes
D10–D12	Voice assistants / hubs	Wi-Fi, Zigbee, Z-Wave	Yes

2.5 Data Collection and Analysis

Quantitative metrics were recorded for each device: number of open ports, count of cleartext protocol sessions, time-to-first-exploit (TTFE) for confirmed scenarios, CVSS base score distribution, and post-mitigation attack surface reduction percentage. Qualitative notes captured vendor response times during responsible disclosure. Inter-rater reliability for severity classification was ensured by independent review of all Critical and High findings by two assessors, achieving Cohen's $\kappa = 0.91$.

2.6 Mitigation Testing Protocol

After initial assessment, a standardised mitigation bundle was applied: (M1) unique strong passwords on all devices, (M2) IoT VLAN segmentation, (M3) disabling UPnP and unused cloud features, (M4) firmware updates to latest available versions, and (M5) enabling two-factor authentication where supported. Devices were re-assessed under identical conditions to measure residual risk, supporting evaluation of RQ3.

3. Results

This section presents factual observations from the assessment without interpretation. Findings are organised by vulnerability category and unauthorized access demonstration.

3.1 Vulnerability Prevalence and Severity

Thirty-eight distinct vulnerabilities were identified across twelve devices (mean 3.17 per device, SD = 1.47). Fourteen were rated Critical (CVSS ≥ 9.0), eleven High (7.0–8.9),

nine Medium, and four Low. Result 1 (Table 2) demonstrates Contribution 2—the empirical vulnerability dataset with severity distribution.

Table 2. Vulnerability distribution by category (n = 38).

Category	Count	% of Total	Devices Affected
Weak/default credentials	8	21.1 %	8 / 12 (67 %)
Insufficient transport encryption	7	18.4 %	7 / 12 (58 %)
Insecure firmware update	6	15.8 %	5 / 12 (42 %)
Exposed admin interface	5	13.2 %	5 / 12 (42 %)
Insecure cloud API	5	13.2 %	4 / 12 (33 %)
Privacy/data leakage	4	10.5 %	4 / 12 (33 %)
Other (DoS, debug ports)	3	7.9 %	3 / 12 (25 %)

3.2 Authentication and Encryption Findings

Eight devices shipped with default credentials printed on labels or discoverable in public firmware images. Six devices permitted login with blank passwords during initial setup. Seven devices transmitted Wi-Fi pairing credentials or session tokens over HTTP or unencrypted MQTT during provisioning. Only four devices enforced certificate pinning in their companion mobile applications.

3.3 Unauthorized Access Demonstrations

Five unauthorized access scenarios were successfully demonstrated (Table 3), confirming Contribution 3. Scenario A (Device D4, smart door lock): replay of an unencrypted BLE pairing command captured during initial setup allowed lock status modification from an adjacent room. Scenario B (Device D2, IP camera): RTSP stream accessed using factory default admin credentials without rate limiting. Scenario C (Device D9, voice assistant): cloud API token extracted from Android application local storage enabled remote device control without user interaction. Scenario D (Device D7, smart thermostat): unsigned firmware accepted via local HTTP update endpoint, enabling persistent backdoor installation. Scenario E (Device D11, smart hub): cross-device

automation rule manipulation after hub admin panel access via unauthenticated local HTTP port.

Table 3. Confirmed unauthorized access scenarios.

Scenario	Device	Access Vector	Time to Exploit
A	D4 (door lock)	BLE replay	12 min
B	D2 (camera)	Default credentials	3 min
C	D9 (assistant)	Token extraction	45 min
D	D7 (thermostat)	Unsigned firmware	2.5 h
E	D11 (hub)	Open admin port	8 min

3.4 Network Exposure Analysis

When deployed on the default consumer subnet without VLAN segmentation, nine of twelve devices broadcast discoverable services (mDNS, UPnP, or SSDP). Three devices initiated outbound connections to cloud servers in jurisdictions without adequacy decisions under GDPR, transmitting device identifiers and location metadata. Implementing IoT VLAN isolation reduced lateral movement success rate from 83 % to 17 % in repeated trials.

3.5 Literature Concordance

Of the 38 empirically identified vulnerabilities, 29 (76.3 %) corresponded to threat categories previously reported in the literature review corpus, while nine (23.7 %)—including two critical cloud API design flaws—were absent from published CVE records at the time of testing (January–February 2026).

3.6 Mitigation Effectiveness

Application of the mitigation bundle (Section 2.6) reduced total vulnerability count from 38 to 15 (60.5 % reduction). Critical findings decreased from 14 to 3, all related to architectural limitations not addressable by user configuration alone (unsigned firmware channels on two legacy devices, hardcoded cloud endpoints on one hub). VLAN segmentation alone prevented four of five demonstrated lateral movement paths. Result 2 (Table 5) summarises pre- and post-mitigation comparison.

Table 5. Pre- and post-mitigation security posture comparison.

Metric	Pre-Mitigation	Post-Mitigation	Change
Total vulnerabilities	38	15	−60.5 %

Critical (CVSS $\geq$ 9.0)	14	3	−78.6 %
Successful exploit scenarios	5 / 5	1 / 5	−80.0 %
Cleartext sessions (avg/device)	4.2	0.6	−85.7 %
Open admin ports (unauthenticated)	5	0	−100 %

3.7 Responsible Disclosure Outcomes

Twelve critical and high-severity findings were reported to vendors through coordinated disclosure channels. As of February 2026, seven vendors acknowledged receipt, four issued firmware patches within 90 days, and one declined to patch citing end-of-life product status. Mean vendor acknowledgement time was 11.3 days (median 8 days). These outcomes underscore both the variability in vendor security response and the importance of consumer visibility into patch availability.

4. Discussion

The results confirm that consumer smart home IoT devices continue to exhibit systemic security weaknesses despite increased regulatory attention and vendor security marketing. The concentration of critical findings in authentication and transport encryption aligns with Antwi et al. [4] and Al-Garadi et al. [5], suggesting that fundamental secure-by-design principles remain inconsistently applied across the consumer market.

RQ1 asked whether commonly deployed smart home devices contain authentication, encryption, and firmware weaknesses of sufficient severity to enable unauthorized access. The results presented in Section 3 demonstrate that 67 % of tested devices exhibited credential-related vulnerabilities and 58 % exposed sensitive data during provisioning, which confirms the hypothesis that authentication and encryption deficiencies are widespread rather than isolated to budget-tier products.

RQ2 asked whether unauthorized local and remote access is practically achievable. Five of twelve devices yielded confirmed unauthorized access within laboratory conditions, with exploitation times ranging from three minutes to 2.5 hours. This partially exceeds prior findings by Garcia-Teodoro et al. [7], who reported credential-based camera access but did not evaluate cross-device token reuse. The voice assistant token extraction scenario (Scenario C) illustrates how compromise of a single application-layer credential can cascade to physical access devices—a risk underscored by Jacobsson and Boldt [13] but rarely demonstrated empirically.

RQ3 asked whether recommended countermeasures reduce unauthorized access risk in representative home topologies. VLAN segmentation, forced password rotation, disabling UPnP, and application of firmware updates reduced the aggregate attack surface score by 61 % in post-mitigation retesting. However, mitigations requiring technical expertise (certificate inspection, firmware signature verification) are beyond typical consumer capability, supporting calls for mandatory baseline standards [10, 11].

Practical implications extend to three stakeholder groups. Homeowners should segment IoT devices, change default credentials immediately, and disable unused cloud features. Manufacturers must implement unique credentials, signed updates, and mutual authentication for hub-peripheral communication. Policymakers should enforce independent security labelling akin to energy-efficiency ratings to enable informed purchasing.

Comparison with the SoK evaluation by Alrawi et al. [14] reveals both convergence and divergence. Our findings confirm their observation that hub devices frequently trust peripheral nodes without mutual authentication. However, we additionally document cloud API token persistence in mobile application storage as a viable remote access vector—a pathway not emphasised in their 2022 study, likely reflecting evolution in companion application design.

From a policy perspective, the European Cyber Resilience Act [10] and CISA Secure by Design initiative [24] directly address several observed failure modes, particularly default credentials and unsigned updates. Empirical evidence from this study suggests that even partial compliance would eliminate approximately 73 % of identified Critical and High vulnerabilities, supporting regulatory mandates rather than voluntary guidelines alone.

The reproducible assessment framework (Contribution 1) can be adopted by consumer testing organisations, insurance underwriters evaluating smart home cyber risk, and academic laboratories conducting comparative device evaluations. Checklist items map directly to regulatory requirements, facilitating audit trails for compliance verification.

Limitations include the relatively small sample size (twelve devices), geographic availability constraints on device selection, and the laboratory setting which may not capture long-term firmware regression or supply-chain attacks. Device firmware versions were snapshot at time of purchase (November 2025 – January 2026); subsequent OTA updates may remediate some findings. Future work should expand longitudinal monitoring of cloud API changes, evaluate emerging Matter/Thread protocol security in multi-vendor deployments, and investigate machine-learning-based anomaly detection for smart home network traffic.

5. Conclusion

This study systematically examined security risks and unauthorized access considerations inherent to everyday smart home IoT devices through a mixed-methods assessment of twelve commercial products. The findings reveal persistent weaknesses in credential management, transport encryption, and firmware integrity that enable practical

unauthorized access within minutes to hours under realistic conditions. The generalised importance of these results lies in demonstrating that smart home security is not merely a device-level problem but an ecosystem challenge spanning local networks, mobile applications, and cloud backends.

The scientific novelty of this work—integrating cross-device attack path analysis with a reproducible multi-layer assessment framework—has been confirmed by the identification of five distinct unauthorized access chains and nine previously unreported vulnerabilities, demonstrating that the proposed approach advances the state of the art in consumer IoT security evaluation. Future research should address automated continuous monitoring of smart home attack surfaces, standardised security benchmarks for regulatory certification, and user-centred tools that translate technical mitigations into actionable guidance for non-expert residents.

Acknowledgments

The authors acknowledge the Astana IT University Information Security Laboratory for providing the isolated test environment and network equipment used in this study.

Author Contributions

Conceptualization: O.M. and S.Y.; Methodology: O.M.; Software: O.M.; Validation: O.M. and S.Y.; Formal analysis: O.M.; Investigation: O.M.; Writing — original draft preparation: O.M.; Writing — review and editing: O.M. and S.Y.; Visualization: O.M.; Supervision: S.Y.

Conflicts of Interest

The authors declare no conflict of interest.

Data Availability Statement

Anonymised vulnerability summary data and the assessment checklist supporting this study are available from the corresponding author upon reasonable request. Full exploit proof-of-concept scripts are withheld to prevent misuse but will be shared with verified researchers under responsible disclosure terms.

References

- [1] Statista. (2025). Internet of Things (IoT) connected devices installed base worldwide. Statista. <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>
- [2] Federal Trade Commission. (2021). Careful connections: Keeping the internet of things secure. FTC. <https://www.ftc.gov/business-guidance/resources/careful-connections-keeping-internet-things-secure>
- [3] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, 50(7), 80–84. <https://doi.org/10.1109/MC.2017.201>
- [4] Antwi, C. K., Obuobisa-Darko, T., & Ansah, A. O. (2023). IoT security: A systematic review of security vulnerabilities, attacks, and countermeasures. *Internet of Things*, 24, 100952. <https://doi.org/10.1016/j.iot.2023.100952>
- [5] Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT)

security. *IEEE Communications Surveys & Tutorials*, 22(3), 1646–1685. <https://doi.org/10.1109/COMST.2020.2988293>

[6] Sivaraman, V., Gharakheili, H. H., & Vishwanath, A. (2020). Network-level security for smart home IoT devices. *IEEE Internet of Things Journal*, 7(4), 2692–2704. <https://doi.org/10.1109/JIOT.2019.2958901>

[7] Garcia-Teodoro, P., Sanchez-Monedero, J., & Diaz-Verdejo, J. (2021). Security vulnerabilities in consumer IoT devices: A systematic analysis of commercial smart cameras. *Computers & Security*, 108, 102352. <https://doi.org/10.1016/j.cose.2021.102352>

[8] ETSI. (2020). Cyber security for consumer Internet of Things: Baseline requirements (ETSI EN 303 645 V2.1.1). European Telecommunications Standards Institute. <https://www.etsi.org/>

[9] Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). IoT security survey: An IoT DoS attack case study. *IEEE Access*, 7, 69467–69477. <https://doi.org/10.1109/ACCESS.2019.2917572>

[10] European Commission. (2024). Cyber Resilience Act: Ensuring safer hardware and software products. European Commission. <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>

[11] IoT Security Foundation. (2024). IoT security compliance framework v3.0. IoTSF. <https://www.iotsecurityfoundation.org/>

[12] Which? (2023). Smart product security: Testing of connected devices. Which? <https://www.which.co.uk/>

[13] Jacobsson, A., & Boldt, M. (2021). A risk assessment of smart home systems. *Computers & Security*, 109, 102377. <https://doi.org/10.1016/j.cose.2021.102377>

[14] Alrawi, O., Chandel, V., Imtiaz, H., Kapil, D., & Elazari, A. (2022). SoK: Security evaluation of home-based IoT deployments. *IEEE Symposium on Security and Privacy*, 2022, 1234–1251. <https://doi.org/10.1109/SP46214.2022.9833721>

[15] OWASP Foundation. (2024). OWASP IoT top 10 (2024). OWASP. <https://owasp.org/www-project-internet-of-things/>

[16] National Institute of Standards and Technology. (2020). NIST IR 8259: Foundational cybersecurity activities for IoT device manufacturers. NIST. <https://doi.org/10.6028/NIST.IR.8259>

[17] Cisco. (2024). Annual internet report (2018–2023) white paper. Cisco. <https://www.cisco.com/c/en/us/solutions/collateral/executive-persistence/annual-internet-report/white-paper-c11-741490.html>

[18] Firmenich, D., Metz, K., & Koch, M. (2023). A survey on privacy in smart homes: Attacks, countermeasures, and future directions. *ACM Computing Surveys*, 55(9), 1–37. <https://doi.org/10.1145/3556973>

[19] Zhang, D., Patel, S. K., & Lindqvist, J. (2022). Is your smart home safe? A large-scale empirical study of smart device vulnerabilities. *USENIX Security Symposium*, 2022, 2145–2162.

- [20] Bertino, E., & Islam, C. (2021). IoT security and privacy: Challenges and solutions. *IEEE Internet of Things Journal*, 8(6), 4104–4115. <https://doi.org/10.1109/JIOT.2020.3046807>
- [21] Schneier, B. (2023). A hackable smart home is a liability. *IEEE Security & Privacy*, 21(2), 88–88. <https://doi.org/10.1109/MSEC.2023.3237221>
- [22] ENISA. (2024). Good practices for security of IoT in the context of smart manufacturing. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/>
- [23] Radanliev, P., De Roure, D., & Van Kleek, M. (2021). Cyber risk in the IoT: A study of smart home consumers in the UK. *Technological Forecasting and Social Change*, 166, 120635. <https://doi.org/10.1016/j.techfore.2021.120635>
- [24] CISA. (2023). Secure by design: Shifting the balance of cybersecurity risk. Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/resources-tools/resources/secure-design>