International Journal of Information Security, Privacy and Digital Forensics Vol. 9, No. 1, June, 2026

Security Architectures for IoT-Based Access Control in Resource-Constrained Settings: A Comparative Study of Abakaliki, Ebonyi State

Ogbu Nwani Henry*[1]
Department of Computer Science, Ebonyi State University, Ebonyi State, Nigeria.
ogbu.henry@ebsu.edu.ng

Ituma Chinagolum[2]
Department of Computer Science, Ebonyi State University, Ebonyi State, Nigeria
chinagolumituma@ebsu.edu.ng

Nwogbaga E. Nweso[3]
Department of Computer Science, Ebonyi State University, Ebonyi State, Nigeria
nwesonwogbaga@yahoo.com

ABSTRACT
The application of smart locker in Ebonyi State, Nigeria, shows that the current Internet of Things (IoT) security guidelines do not fit the contexts in which low-cost systems are deployed. Commonly proposed architectures assume devices that cost more than $10, reliable electric supply, and constant connection. Very few of these assumptions are true in the study context. This paper examines nine publications that came out in the years 2020 through 2025 regarding IoT access control in resource-limited environments. The available evidence is largely based on surveys which provide an overview of previous studies and not field-tested practices. As is evident from the comparison, physical protection (enclosure reinforcement, tamper switches, locks etc.) is not sufficiently mentioned, but the communication protection is mentioned a lot. Both lightweight cryptography and edge computing are suggested but the literature reviewed does not define the means of combining the two for a particular environment like Ebonyi State. None includes the five layers deemed essential here: physical, device, communication, cloud, and application security. This research thus proposes a five-layered framework, and guidance is provided based on unstable electricity, limited processing capacity, low budgets, and intermittent internet access. The principal gap is that layered defence is widely recommended, yet has not been adequately tested where resource constraints are persistent and operationally important.

Keywords: IoT Security, Smart Lockers, Resource-Limited Environments, Layered Security Architecture, Comparative Assessment, Ebonyi State.

1. INTRODUCTION

A smart locker built for Lagos may be planned around dependable 4G service, stable grid electricity, and comparatively secure hardware. Those assumptions cannot be transferred to Izzi Local Government Area or many other parts of Ebonyi State. Nevertheless, the essential duties remain unchanged: authenticate users, record transactions, and detect interference. At one Abakaliki site, usable mobile connectivity averaged about 4.2 hours daily. Grid supply usually arrived in blocks of three to six hours, while replacement batteries could cost more than the locker assembly. These conditions influence every security decision made during development and deployment.

A large proportion of IoT security literature begins from conditions that differ sharply from this

environment. Continuous connectivity is unavailable, electricity is irregular, and components priced above US$10 are often unaffordable. Conventional TLS introduces several communication exchanges, while AES-256 can burden an entry-level microcontroller costing roughly US$2. Cloud-dependent authentication also becomes unavailable immediately a connection fails, which may occur repeatedly during normal operation.

Existing studies offer several disconnected but useful solution components. Lightweight cryptography [3] reduces demand, MQTT-SN [4] supports unstable links, and edge computing [5] limits dependence on remote services. However, the nine publications do not explain how these approaches should be combined for a location with constraints, including 4.2 hours of daily connectivity in Ebonyi State.

The studies also provide little operational guidance for selecting and layering safeguards from local evidence, including network behaviour, processing limits, energy availability, component prices, and realistic maintenance costs.

This paper compares security mechanisms for IoT access control where technical and financial resources are limited. The analysis covers physical, device, communication, cloud, and application layers, after which recommendations are drawn from observed conditions rather than idealised textbook assumptions.

The article proceeds as follows. Section 2 examines relevant scholarship, while Section 3 describes the review procedure. Section 4 compares safeguards across the five layers. Section 5 explains how limited resources intensify familiar threats, and Section 6 presents design considerations. Section 7 interprets the main findings, before Section 8 provides the conclusion and identifies priorities for future investigation.

2. LITERATURE REVIEW

A total of 9 studies that explored IoT security in constrained conditions were studied. The majority reviewed articles which recounted the systems that have been reported, and relatively few directly involved with implementation or long-term field testing.

One of the more extensive surveys is given by Ragothaman et al. [1] who give twelve requirements for IoT access control: granularity, policy administration, interoperability, resource awareness, availability, scalability, etc. They make comparisons between the eight models: DAC, RBAC, ABAC, OrBAC, UCON, CapBAC, BBAC and ReBAC. Their treatment is mostly on a policy level, however, and doesn't consider what the impact of a network outage or power outage will be if it lasts too long. Sicari et al. [2] take the perspective of security and trust in larger IoT ecosystems. The physical layer is once again not discussed in detail, but the physical layer of the DCS is more widespread.

and SIMON can use significantly less energy compared to AES-256 [3]. This is just technically feasible, and the discussion doesn't go on to cloud integration or reliable offline operation. Yusoff et al. [4] take the next step beyond review and instead adopt MQTT communications secured by elliptic-curve cryptography in a smart-home use case. In their prototype they've shown encrypted exchange on cheap hardware, but the connection would need to be relatively stable. This mode of operation is hardly maintainable in many parts of Ebonyi State.

Tripathi and Varadharajan [5] analyze protection in hybrid cloud-edge. They see that while edge processing can enable applications with short response time requirements, there is a risk distribution across multiple edge nodes. Their framework assumes that there are intermittent connections, but it does not specify how the system will behave when it does not have internet access for an extended period of time, for example, a few days. Although their scope is wider, the physical layer is again left outside the detailed analysis.

applications require short response times, but also distribute risk across multiple edge nodes. Xue et al. [9] classify edge-computing access control through the stages of the data lifecycle, including collection, storage, and use. This is a useful perspective, but it does not connect physical interference with corresponding cloud actions. Bessler et al. [8] examine access-control enforcement on Linux-based IoT gateways and document practical policy-implementation difficulties. Their analysis remains concentrated on the gateway and does not address constrained end devices or the protection of equipment against direct physical attack.

The survey titled Securing IoT Edge [13] brings together work on lightweight cryptography, anonymous routing, and improved communication protocols. Although the synthesis is valuable, it does not offer an integrated design covering the five security layers adopted in this study. Bakir et al. [19] propose Caplets, a resource-aware form of capability-based access control. The mechanism adapts authorization to device limitations, but still depends

on sufficient connectivity for distributing and validating capabilities. This dependence remains problematic in the present environment.

Kurte et al. [20] address decentralized IoT operation involving constrained devices and networks. Their work responds to device-level limitations, but omits physical safeguards and gives limited attention to cloud synchronization during repeated outages. Höglund [21] (in a postgraduate thesis) assesses PKI for constrained IoT devices. The results show that PKI can be run on limited hardware, but their research is limited to authentication and not coordinated protection on multiple layers.

The nine studies were aligned with the five layers mentioned in this paper: physical layer, device layer, communication layer, cloud layer and application layer. The disparity became very evident. No one paid sufficient attention to the physical controls of smart lockers, which include Tamper sensing, reinforced enclosures, and secure mounting, and are crucial when smart lockers are placed in public areas that are readily accessible. The most comprehensive coverage was for protection of devices and communications, while individual studies typically covered protection on one or two layers. None of the publications covered all 5.

Three significant gaps were found. First, the reviewed literature focuses primarily on the virtual security of lockers, with little attention paid to physical security, which is a valid concern for unattended lockers. Second, there is no study that makes it clear how the safeguards of the five layers should function. But there are practical issues that are not answered: When a locker enclosure is breached, how will it provide a remote alarm, revoke credentials and initiate local lockdown? Thirdly, there is little information available from the studies based on measured local constraints. They don't say what architecture should do if it's connected for only 4.2 hours each day or if replacement batteries are more expensive than the protected device. The evidence is largely based on laboratory tests, with few long-term field tests under similar conditions to those of Ebonyi State being available.

This paper builds on the work reviewed by structuring the evidence in all five layers and incorporating the little mentioned physical layer and also draws from measurements and experiences of implementation in Ebonyi State. It provides suggestions for well-defined constraint profiles, rather than generic prescriptions created for stable infrastructure and well-funded deployments.

3. RESEARCH METHODOLOGY

The review was conducted following procedures commonly used in systematic studies in computing [10] and [11] and adapted to the nature of evidence in the cybersecurity field, the comparative nature of this study, and the type of evidence being reviewed. Four questions guided the review. Which security mechanisms have been reported for the physical, device, communication, cloud, and application layers of IoT access-control systems? What advantages, limitations, and design trade-offs arise within and between those layers? How have researchers responded to weak hardware, unstable electricity, restricted budgets, and unreliable connectivity? Finally, what unresolved issues prevent the development of an integrated multi-layer architecture suitable for genuinely resource-limited environments?

The database search was conducted in March 2025 across IEEE Xplore, the ACM Digital Library, Scopus, and Google Scholar. Search expressions combined ("IoT" OR "Internet of Things") AND ("access control" OR "authentication") AND ("security architecture" OR "layered security") AND ("resource constrained" OR "lightweight" OR "embedded"). Only peer-reviewed material published from January 2020 to March 2025 was considered.

Five inclusion requirements were applied. A study had to fall within the specified period, be peer reviewed, address security for IoT access control, provide enough technical detail for comparison, and be written in English. Duplicates, non-peer-reviewed sources, papers outside access control, and studies without identifiable security mechanisms were excluded.

Titles and abstracts were screened before potentially relevant studies were read in full. Backward snowballing was then undertaken by examining their reference lists for further eligible material. A standard extraction form was used to record publication details, cover security layers, implemented mechanisms, treatment of resource constraints, and reported limitations.

The data obtained was then coded and analyzed using the five-layer analytical framework.

There are 3 limitations in the method. The search may be limited to English language sources, which could miss relevant studies from China, Brazil and Francophone Africa etc. 2020-2025 is the timeline where recent work is considered, but the foundational work is not included. Lastly, the

emphasis on peer reviewed literature also excludes industry report and technical white papers, which may also include implementation details that are not reported in academic publications.

4. COMPARATIVE ANALYSIS ACROSS FIVE SECURITY LAYERS

This section is provided to help identify the correct level of security for the chosen scenario.

The five layers did not receive the same amount of research attention. Communication protection was mentioned numerous times, while physical security was not discussed much. Most publications dealt with only one or two layers and no publication alluded to the whole framework. This imbalance is shown in figure 1.

using a descriptive coding of the selected studies. The values represent the authors' review judgement and should not be interpreted as a formal bibliometric measure.

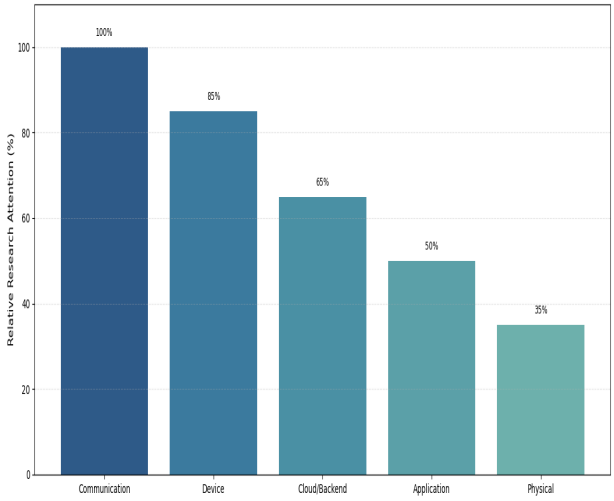


Figure 1. Distribution of Research Attention Across Security Layers

To support consistent comparison, the evidence was arranged within five connected layers: physical, device, communication, cloud, and application security. Their relationship is illustrated in Figure 2.

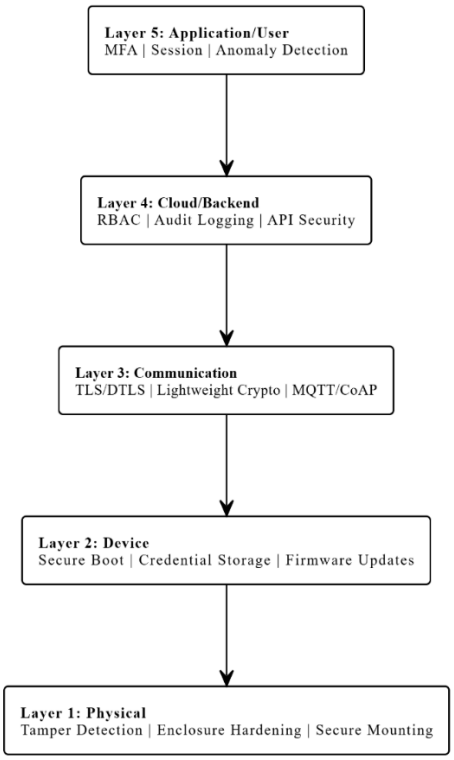


Figure 2. Five-Layer Security Architecture Framework for IoT Access Control

Physical protection is the starting point of direction Previous research mentions tamper sensors, secure enclosures, and tamper resistant installation [3][8][12] but few discuss how these controls can be implemented using low-cost microcontrollers. This omission has an impact because it could be the easiest way to get right into an unlocked public restroom locker. Figure 3 shows a standard lab set-up. It is good for testing purposes but not for the heat, dust, humidity, exposure and vandalism, a unit experience in the field.

Figure 3. Setting up a laboratory for conducting IoT access control testing.

This restriction was also encountered during supervision of student's project in Ebonyi State University project. Some final year teams were able to use micro-switches that are readily available in the country at a negligible cost of about N450 to sense an open enclosure. Their prototypes were able to successfully turn on the LED but nothing else was done: no remote notification was sent and no credential revoked. If you don't take action, a warning that you can see will not keep you safe. Physical

sensors should thus only be chosen once the plan for action, communication pathway and recovery process have been established.

More focus is being given to device-level security – such as secure firmware updates, credential storage and secure boot [13]-[15] – can be considered. However, practice experience shows that there are many aspects that are not always brought to the fore in articles. If you want to enable secure boot on an ESP32 you need to program their eFuse which cannot be reset. One student module broke due to some incorrect configuration and couldn't be used, so the other student's module members turned it off to prevent the others from losing any more module points. Another project stored credentials in software and rotated them daily, but repeated writes produced flash-memory errors during prolonged simulation. A hardware secure element such as the ATECC608A was quoted at ₦6,800 in Abakaliki, while complete student budgets commonly ranged between ₦15,000 and ₦20,000. Such a component was therefore financially unrealistic. Where cost or irreversible configuration leads teams to omit a safeguard, the resulting exposure should be stated and managed openly rather than concealed behind an assumption that protection remains active.

Communication security dominates the reviewed literature. Lightweight cryptography is widely presented as an energy-conscious alternative to AES-256 [3]. Guşiţă et al. [13] examine ciphers including ASCON, PRESENT, SIMON, and SPECK, alongside weaknesses associated with constrained communication protocols such as MQTT-SN. Similar difficulties were observed in projects using SIM800L modules. Table 1 compares representative ciphers, including ChaCha20-Poly1305. In practice, selecting an efficient algorithm is only part of the problem; compatibility with cloud services and their frequent requirement for conventional TLS can determine whether a solution is deployable.

Table 1. Lightweight Cryptographic Ciphers for Resource-Constrained IoT

Cipher	**Key Size**	**Energy Efficiency**	**Primary Application**
ASCON	128-bit	High (NIST standardized)	Authenticated encryption
PRESENT	80-bit	Very high (small hardware footprint)	Low-power sensors
SIMON	48-128-bit	High (ARX structure)	General purpose
SPECK	48-128-bit	High (ARX structure)	Software implementation
ChaCha20-Poly1305	256-bit	Moderate	Stream cipher + MAC

On ESP32-class hardware, a TLS handshake may take 1.8-2.4 seconds and use more than 50 KB of memory [4], making it difficult for cheaper platforms without optimisation. Student systems using SIM800L GSM modules experienced additional instability when supply voltage fell or enclosure temperature exceeded 40 °C. Lightweight algorithms were not abandoned because their cryptographic performance was poor; cloud services required TLS, while software support for alternatives remained limited. Protocol selection should therefore follow measurements of the intended network, hardware, temperature, and power conditions. Laboratory performance cannot be assumed to represent field operation.

Cloud and backend controls, including role-based authorisation, audit trails, and API protection, are discussed extensively [5], [14], [17]. Student implementations nevertheless experienced serious synchronisation delays. As summarised in Table 2, Firebase typically synchronised within one to two seconds under favourable conditions, but required eight to fifteen seconds on weak links. AWS IoT increased from approximately 1.5-2 seconds to 12-25 seconds when connectivity deteriorated.

Table 2. Cloud Synchronization Performance in Student Projects

Platform	**Synchronization Time (good conditions)**	**Synchronization Time (poor conditions)**
Firebase	1-2 seconds	8-15 seconds
AWS IoT	1.5-2 seconds	12-25 seconds

Teams increased request timeouts from 30 to 60 seconds, added local caches and retry queues, and extended JWT validity from 24 hours to between seven and thirty days. The longer validity period weakened security but prevented lockouts during multi-day outages. At moderate transaction rates, ESP32 flash storage could fill within days, yet log rotation was rarely implemented because of complexity. Offline-first operation should be considered a requirement and timeout values should be based on the network behavior and not on platform defaults.

Several studies [17]-[20] take application and user controls (such as multi-factor authentication, session management and anomaly detection) into account. Student trials showed that technically good controls, but not convenient to student use, can fail. Some users, who had complex passwords, had written the same directly on the enclosures of the lockers, and others, who were following the normal procedure, had to send one-time passwords via WhatsApp due to network delays. Biometric verification was turned off due to problems with it in humid weather. Users would tend to ignore scrolling error messages on small screens and repeat the same action over and over again. Authentication needs to be based on conditions in the network, usability of the device, and the actions of the intended users. If not, users will develop workaround solutions that will compromise protection. Similar problems of usability are seen in biometric access control in humid environments [16]. Also, a mathematical model based on adaptive strategy from the access-control approaches discussed in [1] was formulated. It takes into account five indicators, which are combined into a dynamic trust value used in the access decision: the authentication reliability (A), behavioural consistency (B), network stability (N), access frequency (F), and previous security history (H). This model provides the system with the ability to react to the changing operational evidence and not to one specific rule.

Equation (1). Trust Score = $w_1A + w_2B + w_3N + w_4F + w_5H$,

where the five assigned weights have a total value of one.

A graduated response is based on the score. If it is > 0.80, it's okay; if it is between 0.60 and 0.79, then re-authenticate; if it is < 0.60, it's not okay. If a child's score is between 0.40 and 0.59, they can have some privileges, but if the score is below 0.40, the child will be isolated. Its computation can be easily performed on low-resource devices. Weights can be customized based on the situation; in a setup with high security concerns, one might favor weights that reflect the history of security events, while in a network where uptime is paramount, one might opt for weights that better capture network uptime. The decision ranges are given in Table 3.

Table 3. Graduated Response

Trust Score Range	**Access Decision**
0.8 – 1.0	Normal operation (full access)
0.6 – 0.79	Re-authentication required
0.4 – 0.59	Restricted access (limited privileges)
< 0.4	Isolation (no access)

The most critical area of weakness is between layers. It's easy to overlook response chain failures when looking at each layer individually. A micro-switch for one student prototype was used to sense when the enclosure was opened and light an LED. However, tampering took place while a network outage occurred, which meant there was no cloud alert. There was no local lockdown as the secure boot was not included and credentials cannot be revoked because the offline function was not even envisioned. Hence, it was detected as a system but to no effective response. Standalone controls can give the illusion of being secure without actually being secure. Figure 4 shows an example of an unforeseen vulnerability which can permeate multiple layers and jeopardize the architecture

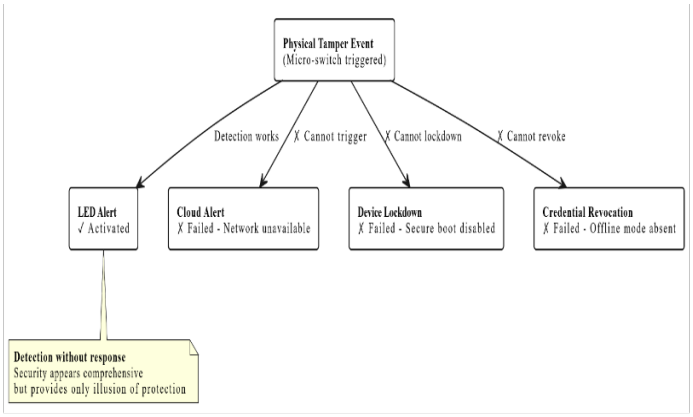


Figure 4. Cross-Layer Integration Failure Cascade

Future designs should define how an event at one layer initiates responses elsewhere. Where a constraint weakens one layer, deliberate

compensating controls must be provided within another.

5. THREAT LANDSCAPE

Limited resources don't mean new attacks, but it does mean more often and more severe risks of attack. The pattern is summarised in table 4. Limited memory can be a reason for not logging and weak processing power may lead to a lower cryptographic protection. During periods of energy scarcity, operators might be tempted to turn off protections, intermittent network access can result in uncontrolled off networks operations, and low-cost hardware often doesn't include security elements for protected key storage.

Table 4. Risk Amplification from Resource Constraints

Constraint	**How It Amplifies Risk**	**Affected Layers**
Limited processing	May force use of weaker cryptography	Device, Communication
Insufficient memory	Prevents comprehensive logging	Device, Cloud
Power limitations	May lead to security features being disabled	Device, Communication
Intermittent connectivity	May force insecure offline modes	All layers
Low-cost hardware	Eliminates secure elements	Physical, Device

This trade-off was shown by student experiments. Security vs. acceptable response time became an issue with AES-256, as it caused noticeable delays with transactions above two per minute. If a limitation has a negative impact on one layer, then another layer should compensate for it. Without implementing mitigation measures, however, a recognition of an exposure is not "effective risk management.

6. DESIGN CONSIDERATIONS

Power constraints: Lightweight cryptography is recommended as for battery operated devices [3]. Students who tried to use ESP32 deep sleep (10 uA or so) on tamper monitoring discovered that in some situations, an interrupt-based wakeup was not reliable. With continuous sensing, batteries would deplete in days. The energy expenditure on cryptographic operations should be commensurate with the available energy budget, and the wake-up behaviour should be evaluated many times in realistic operating conditions.

Hardware restrictions: IoT devices are categorized according to the memory and computing power they have. The ESP32-WROOM-32D used has 520 KB of RAM, a factor that puts it in the middle tier – or Class 1 and Class 2 – of devices. While TLS is possible, it is still challenging to implement. Table 5 provides a range of options: an Arduino Uno with 2 KB would not work with TLS, an optimised ESP32 might be able to support TLS, and a Raspberry Pi Zero with 512 MB could support TLS with plenty of space to spare. The selection of hardware should be based on the security functions that are required; unavoidable weaknesses should be noted.

Table 5. Hardware Capability Mapping for IoT Devices

Device	**RAM**	**TLS Feasibility**
Arduino Uno	2KB	Not feasible
ESP32	520KB	Theoretically possible with optimization
Raspberry Pi Zero	512MB	Fully feasible

Network unreliability: Local authentication when no remote services is available [5] [21]. Delayed transmission, longer timeouts, and cryptographically verified credential caches were implemented on student's system. The idea is simple: if connectivity can't be assured, the architecture has to be secure and operational when the connectivity is unavailable.

Cost-security trade-offs: Secure elements can be expensive and can take up a big portion of the project budget, in order to highly secure credentials. The ATECC608A cost in local currency was quoted at ₦6,800 while the total budget of the students was approximately ₦15,000- ₦20,000. It was not observed in any of the teams. Table 6 indicates that there was partial support for free TLS/HTTPS and tamper switches costing ₦450 were prevalent. Although it was more beneficial, the security element was not there. Safeguards should be in proportion to value and risk of assets being safeguarded. Ideal control measures may not always be feasible and

alternative exposure and corrective action must be accepted and recorded.

Table 6. Cost-Security Trade-Offs in Student Projects

Mechanism	Local Cost	Security Benefit	Student Adoption
Hardware secure element	₦6,800	Very high	None observed
TLS/HTTPS	Free	High	Partial
Tamper detection switch	₦450	Moderate	Common

The Design Principle, there are five lessons that are gleaned from the design principles. Before choosing safeguards, check the local infrastructure and the user conditions, as laboratory test results can be misleading. Secondly, make sure to have offline security when connection is not guaranteed. Record risks where a perfect control is not possible due to technical or financial constraints. Fourth, make up for a weak layer with controls in other layers. Fifth, test the system under real world power, temperature, network and usage circumstances as well as under lab conditions.

7. DISCUSSION

The main findings of the research are that: When it comes to IoT security in constrained environments, the research mostly focuses on communication security and much less on physical security. Material constraints such as limited processors, small memory, unreliable power, unreliable networks, and limited budgets impact the type of controls that can be implemented and maintained. Therefore, the traditional notions of encryption, logging, cloud access and authentication may be wrong. The second one is that there is no cross layer coordination. The publications reviewed are not sufficient in describing what happens if there is a physical tamper, the local locking, remote notification, audit record, or revocation of credentials. Layers are usually considered as distinct technical areas. Guidance around measurable limits (e.g. 4.2 hours of daily connectivity or a component cost of N6,800) is also hard to come by. Most evidence are from the laboratory and field validation in similar settings as Ebonyi State is still a rarity.

Implications for researchers: The need for cross-layer integration should be the most obvious item for future research. Research should clarify the flow of events, decisions, and instructions between layers and the approach for resolving conflicts between the different results of separate controls. Recommendations should also be correlated with hardware, memory, energy, connectivity, and cost reported. Prototypes are not just conceptual arguments but have to be given a thorough test in the context of environments for which they are designed.

Implications for practitioners: Equipment publicly accessible should not only provide an indicator but also an actionable local response and be tamper sensing. For systems that use unreliable networks, it is essential that there is verified local authentication and secure delayed synchronisation. If budgets dictate that stronger controls are impossible, a weaker form of cryptography and/or compensating controls are better than turning off security for no apparent reason. Document compromises, residual exposure and recovery procedures for small projects. If the preferred means of protection is not possible then protection at another level should be intentionally enhanced.

CONCLUSION

The review covered nine studies, and categorized the evidence under five interrelated levels: physical security, device security, communication security, cloud security, and application security**.**

There was considerable variation in coverage. The protection of communication was given heavy consideration, while physical protection was more or less ignored. There were also changes in what could be implemented due to the resource constraints and no reviewed framework had all 5 layers.

Five layers of security controls are presented for considering differences and similarities, the influence of local constraints on the choice of implementation and integration of the security controls across layers is highlighted as a research gap, and practical considerations are suggested for deployments with limited resources.

Future research should focus on 'integrated' architecture, guidance in relation to the constraints, and field validation. Design for local conditions that have been measured and document security risk(s) that must be accepted.

When IoT systems are deployed in environments which have stringent practical limitations, assuming ideal security by default will create installations that look secure but are operationally insecure. However, these systems can also be unsuccessful during routine outages, maintenance delays, tampering attempts and user workarounds even though all their security controls may look technically fine in practice.

REFERENCES

[1] K. Ragothaman, Y. Wang, B. Rimal, and M. Lawrence, "Access control for IoT: A survey of existing research, dynamic policies and future directions," Sensors, vol. 23, no. 4, p. 1805, Feb. 2023.

[2] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "Security and trust in IoT ecosystems: A survey," Journal of Information Security and Applications, vol. 68, p. 103207, 2022.

[3] B. Bilgin, A. Sahin, and S. Tekinay, "Lightweight cryptography for resource-constrained IoT devices: A survey," Journal of Network and Computer Applications, vol. 160, p. 102634, 2020.

[4] Z. Y. M. Yusoff, M. K. Ishak, L. A. B. Rahim, and M. S. M. Asaari, "Improving smart home security via MQTT with elliptic curve cryptography," Computer Systems Science and Engineering, vol. 48, no. 6, pp. 1669–1697, 2024.

[5] A. Tripathi and V. Varadharajan, "Security frameworks for hybrid cloud–edge IoT architectures," Computers & Security, vol. 124, p. 102929, 2023.

[6] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Keele University, Technical Report EBSE-2007-01, 2007.

[7] C. Okoli and K. Schabram, "A guide to conducting a systematic literature review of information systems research," Sprouts: Working Papers on Information Systems, vol. 10, no. 26, 2010.

[8] M. Bessler, P. Sangster, R. Upadrashta, and T. O'Connor, "Hardening the Internet of Things: Toward designing access control for resource constrained IoT devices," in Proceedings of the 17th Workshop on Cyber Security Experimentation and Test (CSET 2024), ACM, 2024.

[9] T. Xue, Y. Zhang, Y. Wang, W. Wang, S. Li, and H. Zhang, "Edge computing for IoT: Novel insights from a comparative analysis of access control models," Computer Networks, vol. 270, article no. 111468, Oct. 2025.

[10] F. K. Hussain, E. Chang, and O. K. Hussain, "Cybersecurity readiness of IoT based access control systems: Models and implications," Internet of Things, vol. 15, article no. 100467, 2021.

[11] B. M. Fernandes, J. J. P. C. Rodrigues, and M. Al Mhiqani, "Secure token based authentication for distributed IoT systems," Computers & Security, vol. 92, article no. 101754, 2020.

[12] F. Al Turjman, "Security and privacy in Internet of Things (IoT): Models, algorithms, and challenges," IEEE Internet of Things Journal, vol. 9, no. 15, pp. 12334–12358, 2022.

[13] B. Guşiţă, A. A. Anton, C. S. Stângaciu, D. Stănescu, L. I. Găină, and M. V. Micea, "Securing IoT edge: A survey on lightweight cryptography, anonymous routing and communication protocol enhancements," International Journal of Information Security, vol. 24, article no. 149, 2025.

[14] A. Jukan, A. Klein, and R. Bala, "Authentication & access control mechanisms to secure distributed IoT environments," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2820–2843, 2020.

[15] J. Yang, L. Zhao, and Q. Li, "Biometric authentication in IoT-enabled smart environments: Privacy and security perspectives," Future Generation Computer Systems, vol. 115, pp. 366–378, 2021.

[16] B. Salem and M. Hasan, "Evaluating biometric authentication for IoT access control," Journal of Information Security and Applications, vol. 64, article no. 103089, 2022.

[17] T. N. Dinh, Z. Aung, and D. Kim, "Time based one time passwords and anomaly detection for secure access in IoT," Sensors, vol. 23, no. 12, article no. 5032, 2023.

[18] I. Zerraza, "Lightweight Authentication for IOT Edge Devices," Informatica, vol. 48, no. 18, 2024. DOI: 10.31449/inf.v48i18.6012

[19] F. Bakir, C. Krintz, and R. Wolski, "Caplets: Resource aware, capability-based access control for IoT," in 2021 IEEE/ACM Symposium on Edge Computing (SEC), IEEE, 2021.

[20] R. Kurte, Z. Salcic, and K. I-K. Wang, "Supporting constrained devices and networks in

the decentralised Internet of Things," Internet of Things, vol. 30, article no. 101496, 2025.

[21] J. Höglund, "Public Key Infrastructure and its applications for resource-constrained IoT," Doctoral thesis, Department of Information Technology, Uppsala University, Sweden, 2023. Available at: http://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-495320