ISSN 2320-9984
Volume 6 Issue 1 | March 2018 ISSN: 2320-9984 (Online)
International Journal of Modern Engineering & Management Research
Website: www.ijmemr.org

Security and Privacy in the Internet of Things: A Systematic Review

Rupesh Kumar Dharne
Lecturer
Kalaniketan Polytechnic College, sss
Jabalpur, (M.P.) [India]
Email: rk.dharne@gmail.com

Shuchita Mudgil
Lecturer
Kalaniketan Polytechnic College,
Jabalpur, (M.P.) [India]
Email: shuchitamudgil@gmail.com

Abstract:—*The rapid spread of IoT devices has led to complex interconnected environments, but at the same time it brings with it important challenges in data protection, privacy and security. This review brings together studies and industry reports to discuss IoT security. It includes basic requirements like confidentiality, integrity, authentication, access control, availability and privacy as well as common threats including unauthorised access, DoS attacks, malware, RFID cloning, buffer overflows, firmware modification, vehicle hacking, and data breaches. Countermeasures considered are lightweight cryptography, mutual authentication, capability-based access control, federated security, hardware-accelerated authentication, memory safety frameworks (DISARM, nesCheck) incident response (Kinesis) and secure protocols for drones and vehicles. Main issues are: resource constrained devices, firmware vulnerabilities, unsecured updates, heterogeneous architectures, scalability, deployment gaps and non-satisfactory traditional solutions. The review finishes with open research topics and future perspectives for secure and privacy preserving the IoT systems.*

1. INTRODUCTION

IoT is a paradigm change, connecting billions of devices into interconnected ecosystems. An early investigation (Roman et al., 2011) has shown that the combination of wireless sensors, RFID and cloud computing introduces vulnerabilities that typical security solutions do not address. According to Harini et al. (2017), privacy and security is important for the success of IoT and so, effective authentication and data protection are required. From an economic perspective, McKinsey (Manyika et al., 2013) acknowledges IoT as a revolutionary technology that can create trillions of dollars per year in health care, manufacturing, and smart cities, but to achieve this potential, basic security challenges must be addressed. Mashal et al. (2015) study user-device interaction paradigms (direct, cloud-mediated, service-oriented) and emphasise security, privacy, scalability and interoperability as main underlying challenges. This review summarises findings from forty seminal studies (1987-2016) and industry frameworks and real-world attack reports to evaluate IoT security and privacy. A number of research on security requirements of IoT systems have been discovered. Confidentiality - securing sensitive information in transmission and storage is highlighted by Farooq et al. (2015), Abomhara and Køien (2014) and Roman et al. (2011). Integrity, which prevents unauthorised data change, is addressed by Farooq et al. (2015), Abomhara and Køien (2014) and Zhao et al. (2011). Continuous access to services and protection against DoS attacks is covered in Farooq et al. (2015), Abomhara and Køien (2014) and Sicari et al. (2015).

Table 1: Security Requirements Across Reviewed Studies

Security Requirement	Key Studies	Summary of Emphasis
Confidentiality	Farooq et al. (2015), Abomhara and Køien (2014), Roman et al. (2011)	Protecting sensitive information from unauthorized access during transmission and storage
Integrity	Farooq et al. (2015), Abomhara and Køien (2014), Zhao et al. (2011)	Preventing unauthorized data modification; ensuring data accuracy
Availability	Farooq et al. (2015), Abomhara and Køien (2014), Sicari et al. (2015)	Guaranteeing uninterrupted access to IoT services; DoS mitigation
Authentication	Zhao et al. (2011), Lee et al. (2014), Challa et al. (2017), Singla et al. (2015)	Verifying identities of devices, users, and services before communication
Access Control	Mahalle et al. (2013), Xie and Wang (2014), Bertino (2016), Nehme et al. (2013)	Ensuring only authorized entities access IoT resources; fine-grained and continuous enforcement
Privacy Preservation	Bertino (2016), Harini et al. (2017), Shebaro et al. (2014)	Safeguarding personal information; permission and call flow analysis
Trust Management	Roman et al. (2011), Leo et al. (2014), Sicari et al. (2015)	Establishing trust across heterogeneous, multi-domain environments
Memory Safety	Habibi et al. (2015), Midi et al. (2016)	Preventing buffer overflow and memory corruption vulnerabilities
Firmware Integrity	Costin et al. (2014), Cui et al. (2010)	Ensuring firmware authenticity and preventing malicious modifications

Authentication is investigated by Zhao et al. (2011), Lee et al. (2014), Challa et al. (2017) and Singla et al. (2015) where identities are verified before communication. Mahalle et al. (2013), Xie and Wang (2014), Bertino (2016) and Nehme et al. (2013) study access control, which is the providing of resource access to authorised entities by using fine-grained enforcement. Bertino (2016), Harini et al. (2017) and Shebaro et al. (2014) deal with privacy preservation, i.e. protection of personal information. Roman et al. (2011), Leo et al. (2014) and Sicari et al. (2015) studied trust management in heterogeneous contexts. Additionally, memory safety (Habibi et al., 2015; Midi et al., 2016) avoids buffer overflows and firmware integrity (Costin et al., 2014; Cui et al., 2010) guarantees authenticity and avoids malicious changes.

2. FUNDAMENTAL SECURITY REQUIREMENTS AND THREATS

2.1 Core Security Requirements

The literature provides a set of basic security requirements that IoT devices should meet. Abomhara and Køien (2014) pointed out the main needs as confidentiality, integrity, authentication, access control, availability and privacy protection. We provide a systematic classification of these criteria, and explain that security should be regarded as a core design requirement, rather than an add-on. Similarly, Farooq et al. (2015) base their analysis on the Confidentiality, Integrity and Availability (CIA) model, while Oracevic, Dilekand Ozdemir (2017) emphasise on CIA triad as the fundamental pillars of IoT security.

Roman et al. (2011) say that authentication verifies the validity of devices

Table 2: Common IoT Security Threats and Associated Studies

Threat Category	Specific Threats	Studies Reporting
Network attacks	Eavesdropping, man-in-the-middle, DoS, replay attacks	Farooq et al. (2015), Zhao et al. (2011), Lee et al. (2014)
Device-level attacks	RFID tag cloning, tampering, physical attacks	Farooq et al. (2015), Oracevic et al. (2017)
Software attacks	Malware, viruses, code injection	Zhang et al. (2014), Bansal (2014)
Firmware attacks	Malicious modifications, hardcoded credentials, outdated components	Cui et al. (2010), Costin et al. (2014)
Memory corruption	Buffer overflow, memory safety violations	Habibi et al. (2015), Midi et al. (2016)
Vehicle attacks	Unauthorized control of braking, steering, acceleration	Wright (2011)
Identity-based attacks	Impersonation, identity theft, spoofing	Zhao et al. (2011), Mahalle et al. (2013)
Data-related attacks	Data breach, data manipulation, privacy violation	Bertino (2016), Shebaro et al. (2014)
Access-related attacks	Unauthorized access, privilege escalation	Yousuf et al. (2015)
Cryptocurrency attacks	Botnet mining, spam distribution	Bansal (2014)

and users, confidentiality prevents unlawful access to sensitive information, integrity prevents the alteration of data while in transit, privacy protects personal and organisational information, and availability guarantees continuous access to IoT services. Table 1 maps security requirement to the studies focusing on them.

2.2 Major Security Threats

The research studied shows a common set of hazards to IoT setups. Common issues include unauthorised access, eavesdropping, DoS assaults, malware infections, identity theft and data breaches, according to Abomhara and Køien (2014). Farooq et al. (2015) includes RFID tag cloning and network level threats. Impersonation assaults and replay attacks are discussed by Zhao et al. (2011), Lee et al. (2014).

2.3 Real-World Attack Evidence

Firmware and embedded devices are attack vectors. Cui et al. (2010) showed that malicious firmware changes can overcome security measures and take control of embedded systems, emphasising the need for firmware integrity testing and secure updates. Costin et al. (2014) detected hardcoded credentials, obsolete components, and cryptographic flaws in thousands of devices from various suppliers. Wright (2011) explained in vehicle hacking how linked cars create new attack surfaces that can exploit software weaknesses to control braking, steering and acceleration, endangering human life. Bansal (2014) has stated that botnet and malware campaigns are targeting household appliances with weak default passwords to mine cryptocurrencies and distribute spam. Industry vulnerability studies corroborate these risks: Over 70% of IoT devices

Table 3: Layer-Specific IoT Security Vulnerabilities and Countermeasures

Layer	Function	Vulnerabilities	Example Threats	Proposed Counter-measures
Perception layer	Data sensing and collection using RFID, sensors	Physical tampering, cloning, eavesdropping	RFID tag cloning, node capture, side-channel attacks	Lightweight encryption, physical unclonable functions (PUFs)
Network layer	Communication and data transmission	Interception, DoS, routing attacks	Eavesdropping, sinkhole attacks, selective forwarding	Secure routing protocols, IPSec, DTLS, SDN-based security, HAT
Middleware layer	Data processing, service management	Unauthorized access, service availability threats	API abuse, data integrity attacks	Capability-based access control, continuous access control
Application layer	End-user services	Privacy breaches, insecure interfaces	Malware, cross-site scripting, poor authentication	Application firewalls, secure coding Droid-Detector

reviewed by Rawlinson (2014) have vulnerabilities such weak passwords, unsecured web interfaces and poor encryption. Patton et al. (2014) found default passwords and misconfigured services.

3. LAYER-SPECIFIC VULNERABILITIES

Many research analyses IoT security layer by layer. Farooq et al. (2015) identify vulnerabilities and threats in the generic IoT architecture's perception, network, middleware and application layers. Layer-specific vulnerabilities and responses are in Table 3.

Mashal et al. (2015) examined three user-object interaction paradigms: direct, cloud-mediated, and service-oriented, each with security concerns. Cloud mediation challenges trust and data sovereignty. Direct exposure allows local attacks. Service-oriented designs increase API exposure and attack surface. Security, privacy, scalability, interoperability, and resource management are major considerations. Sicari et al. (2015) identified scalability, heterogeneity, and dynamic network conditions as the main obstacles and stated that future IoT systems need adaptive, context-aware frameworks. Bertino (2016) also mentioned the limits of typical security procedures in varied IoT environments and recommended scalable and adaptive frameworks. Roman et al. (2011) suggested flexible security architectures and strong trust management systems to address these issues.

4. SECURITY SOLUTIONS AND COUNTERMEASURES

To secure IoT, researchers suggest cryptography, authentication, memory safety, access control, federated architectures, incident response, and privacy analysis. For public-key operations on constrained devices, lightweight cryptography uses ECC (Koblitz, 1987), while Challa et al. (2017) used biometric authentication with ECC for quick key creation. White-box cryptography secures keys in untrusted situations using space-hard cyphers and dynamic key transformations (Boyd and Isobe, 2015; Won et al., 2016). Mutual authentication (Zhao et al., 2011) provides two-way identity verification, whereas lightweight authentication (Lee et al., 2014) decreases computational and energy needs and avoids replay and impersonation threats. DISARM (Habibi et al., 2015) mitigates buffer overflows with low overhead, and nesCheck (Midi, 2016) integrates static

analysis with dynamic instrumentation for wireless sensor networks. The IACAC framework, secure delegation between domains, item-level control, and context-adaptive continuous access enforcement are all access control mechanisms. Federated security architectures (Leo et al., 2014) distribute trust across domains to prevent single points of failure, while mediation systems (Castrucci et al., 2012) enable secure cross-organizational communication. Kinesis (Sultana et al., 2014) detects and mitigates hazards in sensor networks for incident response. Mobile device authentication and integrity are handled by a secure drone communication protocol (Won et al., 2015). Android IoT privacy analysis is supported by DroidDetector (Shebaro et al., 2014). Finally, dynamic policy enforcement (Neisse et al., 2014) and layered security architectures (Farooq, 2015; Sicari, 2015; Harini, 2017) highlight security integration and threat response.

5. OPEN CHALLENGES AND RESEARCH GAPS

Many research found IoT security problems. Low device resources constrain standard security solutions, requiring lightweight methods (Zhang et al., 2014; Abomhara and Køien, 2014; Yousuf et al., 2015). Despite memory safety solutions like DISARM (Habibi et al., 2015) and nesCheck (Midi, 2016), numerous obsolete devices still have buffer overflow vulnerabilities. Firmware and supply chain security are major concerns. Costin et al. (2014) and Cui et al. (2010) found hardcoded credentials, obsolete components, and no cryptographic signature verification for updates, allowing malicious firmware to install. Vehicular IoT security is crucial; Wright (2011) warned against illegal braking and steering system manipulation. Due to old codebases and long lifecycles, connected car architectures are immature despite hardware-accelerated authentication (Singla et al., 2015). Scalability and standardisation gaps continue, according to Yousuf et al. (2015) and Bertino (2016), who argue for cross-platform frameworks. There exist federated models (Leo et al., 2014), but no common trust protocols. Privacy protection remains a priority (Bertino, 2016; Abomhara and Køien, 2014), while DroidDetector (Shebaro et al., 2014) is limited to Android platforms. Trust management in several sectors is unresolved (Leo et al., 2014; Anggorojati, 2012). Key management for billions of devices remains challenging (Abomhara and Køien, 2014). White-box cryptography (Boyd and Isobe, 2015; Won et al., 2016) offers key security, but distribution and lifecycle management difficulties remain unresolved. Deployment differences are clear: Patton et al. (2014), Bansal (2014), and Rawlinson (2014) note that production systems lack basic security protocols. Real-time, mission-critical security requires robust security and low latency (Singla et al., 2015; Wright, 2011). Kinesis (Sultana et al., 2014) works for wireless sensor networks, but scalable automatic responses and SIEM/ SOAR integration for IoT deployments are still developing.

6. CONCLUSION AND FUTURE DIRECTIONS

This review includes various studies on foundational cryptography (Koblitz, 1987), firmware security (Costin et al., 2014; Cui et al., 2010), automotive security (Wright, 2011), memory safety (Habibi et al., 2015; Midi, 2016), access control, incident response, hardware acceleration, drone communication, and 5G enablers. Multiple major findings are confirmed in this literature. Resource constraints, variety, and scalability make traditional security solutions unsuitable for IoT. Most embedded systems include firmware vulnerabilities such hardcoded credentials, outdated components, and insufficient security upgrades (Costin et al., 2014; Cui, 2010). Wright (2011) showed that linked cars can be hacked to control braking, steering, and acceleration, posing life-threatening risks. Despite DISARM and nesCheck, buffer overflows occur, making memory safety crucial (Habibi et al., 2015;

Midi, 2016). Dynamic data streams require constant, rigorous access control (Nehme et al., 2013). Mission-critical vehicular IoT requires hardware acceleration and real-time authentication (Singla et al., 2015). Empirical study shows that theoretical frameworks and practical application differ (Patton et al., 2014; Rawlinson, 2014). The economic forces described by Manyika et al. (2013) emphasise the need to solve these issues. As the IoT grows in healthcare, smart cities, transportation and critical infrastructure, lightweight cryptography, secure firmware, memory safety, continuous access control, hardware acceleration and automated incident response are the best ways to secure the design.

REFERENCES:

[1] Abomhara, M., and Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. In *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)* (pp. 1–8). IEEE.

[2] Anggorojati, B., Mahalle, P. N., Prasad, N. R., and Prasad, R. (2012). Capability-based access control delegation model on the federated IoT network. In *2012 15th International Symposium on Wireless Personal Multimedia Communications (WPMC)* (pp. 604–608). IEEE.

[3] Bansal, K. (2014, March). Linux worm targets internet-enabled home appliances to mine cryptocurrencies. *The Hacker News*.

[4] Bertino, E. (2016). Data security and privacy in the IoT. In *Proceedings of the 19th International Conference on Extending Database Technology (EDBT)* (pp. 639–640).

[5] Boyd, A., and Isobe, T. (2015). White-box cryptography revisited: Space-hard ciphers. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15)* (pp. 1058–1069). ACM.

[6] Castrucci, M., Neri, A., Caldeira, F., Aubert, J., Khadraoui, D., Aubigny, M., and others. (2012). Design and implementation of a mediation system enabling secure communication among critical infrastructures. *International Journal of Critical Infrastructure Protection, 5*(3–4), 86–97.

[7] Challa, S., Das, A. K., Odelu, V., Kumar, N., Kumari, S., Khan, M. K., Choo, K.-K. R., and Park, Y. (2017). Secure signature-based authenticated key establishment scheme for future IoT applications. *IEEE Access, 5*, 3028–3043.

[8] Costin, A., Zaddach, J., Francillon, A., and Balzarotti, D. (2014). A large-scale analysis of the security of embedded firmwares. In *Proceedings of the 23rd USENIX Security Symposium (USENIX Security '14)* (pp. 95–110). USENIX Association.

[9] Cui, A., Costello, M., and Stolfo, S. J. (2010). When firmware modifications attack: A case study of embedded exploitation. In *Proceedings of the 17th Annual Network and Distributed System Security Symposium (NDSS 2010)*. Internet Society.

[10] Farooq, M. U., Waseem, M., Khairi, A., and Mazhar, S. (2015). A critical analysis on the security concerns of Internet of Things (IoT). *International Journal of Computer Applications, 111*(7), 1–6.

[11] Habibi, J., Panicker, A., Gupta, G., and Bertino, E. (2015). Disarm:

Mitigating buffer overflow attacks on embedded devices. In S. Foresti, G. Persiano, and G. Ventre (Eds.), *Network and System Security: 9th International Conference, NSS 2015* (pp. 112–129). Springer.

[12] Harini, S., Jothika, K., and Jayashree, K. (2017). A survey on privacy and security in Internet of Things. *International Journal of Innovations in Engineering and Technology, 8*(1), 129–134.

[13] Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation, 48*(177), 203–209.

[14] Lee, Y.-Y., Lin, W.-C., and Huang, Y.-H. (2014). A lightweight authentication protocol for Internet of Things. In *2014 International Symposium on Next-Generation Electronics (ISNE)* (pp. 1–2). IEEE.

[15] Leo, M., Battisti, F., Carli, M., and Neri, A. (2014). A federated architecture approach for Internet of Things security. In *2014 Euro Med Telco Conference (EMTC)* (pp. 1–5). IEEE.

[16] Mahalle, P. N., Anggorojati, B., Prasad, N. R., and Prasad, R. (2013). Identity authentication and capability based access control (IACAC) for the Internet of Things. *Journal of Cyber Security and Mobility, 1*(3), 309–348.

[17] Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., and Marrs, A. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy*. McKinsey Global Institute.

[18] Mashal, I., Alsaryrah, O., Chung, T.-Y., Yang, C.-Z., Kuo, W.-H., and Agrawal, D. P. (2015). Choices for interaction with things on Internet and underlying issues. *Ad Hoc Networks, 28*, 68–90.

[19] Midi, D., Peyer, M., and Bertino, E. (2016). *nesCheck: Static analysis and dynamic instrumentation for nesC memory safety*. Purdue University Technical Report.

[20] Nehme, R. V., Lim, H., and Bertino, E. (2013). Continuous access control enforcement in dynamic data stream environments. In *Proceedings of the Third ACM Conference on Data and Application Security and Privacy (CODASPY '13)* (pp. 243–254). ACM.

[21] Neisse, R., Steri, G., and Baldini, G. (2014). Enforcement of security policy rules for the Internet of Things. In *2014 IEEE 10th International Conference on Wireless* and Mobile Computing, Networking and Communications (WiMob) (pp. 165–172). IEEE.

[22] Oracevic, A., Dilek, S., and Ozdemir, S. (2017). Security in Internet of Things: A survey. In 2017 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1–6). IEEE.

[23] Patton, M., Gross, E., Chinn, R., Forbis, S., *Walker, L., and Chen, H. (2014). Uninvited connections: A study of vulnerable devices on the Internet of Things (IoT). In 2014 IEEE Joint Intelligence and Security Informatics Conference (JISIC) (pp. 232–235). IEEE.*

[24] Rawlinson, K. (2014). HP study reveals 70 percent of Internet of Things devices vulnerable to attack. *HP News*.

[25] Roman, R., Najera, P., and Lopez, J. (2011). Securing the Internet of Things. *Computer, 44*(9), 51–58.

[26] Shebaro, B., Oluwatimi, O., Midi, D., and Bertino, E. (2014). DroidDetector: Android call flow and permission usage analysis on data privacy. In *Proceedings of the 25th International Workshop on Database and Expert Systems Applications (DEXA 2014)* (pp. 188–192). IEEE.

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

[28] Singla, A., Mudgerikar, I., Papapanagiotou, I., and Varvarigou, A. (2015). HAT: Hardware-accelerated authentication for Internet of Things in mission-critical vehicular networks. In *2015 IEEE Military Communications Conference (MILCOM 2015)* (pp. 1298–1304). IEEE.

[29] Sultana, S., Midi, D., and Bertino, E. (2014). Kinesis: A security incident response and prevention system for wireless sensor networks. In *Proceedings of the 12th ACM Conference on Embedded Networked Sensor Systems (SenSys '14)* (pp. 148 –162). ACM.

[30] Won, J., Seo, J., and Bertino, E. (2015). A secure communication protocol for drones and smart objects. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (ASIACCS '15)* (pp. 249–260). ACM.

[31] Won, J., Seo, J., and Bertino, E. (2016). *White-box attack-resistant dynamic block cipher for vehicular networks*. Purdue University Technical Report.

[32] Wright, A. (2011). Hacking cars. *Communications of the ACM, 54* (11), 18–19. https://doi.org/10.1145/2018396.2018409

[33] Xie, Y., and Wang, D. (2014). An item-level access control framework for inter-system security in the Internet of Things. *Applied Mechanics and Materials, 530–531*, 1430–1433.

[34] Yousuf, T., Mahmoud, R., Aloul, F., and Zualkernan, I. (2015). Internet of Things (IoT) security: Current status, challenges and countermeasures. *International Journal for Information Security Research, 5*(4), 608–616.

[35] Zhang, Z.-K., Cho, M. C. Y., Wang, C.-W., Hsu, C.-W., Chen, C.-K., and Shieh, S. (2014). IoT security: Ongoing challenges and research opportunities. In *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications (SOCA)* (pp. 230–234). IEEE.

[36] Zhao, X. S., Wang, J., Long, X., and Hu, T. (2011). A novel mutual authentication scheme for Internet of Things. In *2011 International Conference on Modelling, Identification and Control (ICMIC)* (pp. 563–566). IEEE.