The Current Landscape of IoT Security, a Survey Paper Across Novel Methods in the Field

HARRY HILLSDOWNLEY

ABSTRACT

This survey paper examines the current state of security across Internet of Things (IoT) devices. We aim to approach security across IoT by identifying fundamental security objectives, implementation challenges, and solutions for these challenges currently being researched in the field. This paper identifies confidentiality and integrity as primary concerns for IoT device environments due to resource constraints, the heterogeneity of the field, and lack of standardization, which make it possible for attackers to exploit a large attack surface across multiple networks.

This paper aims to review technical approaches to secure IoT systems, including Symmetric Homomorphic Mapping for data aggregation without decryption, blockchain implementation for trust mechanisms, lightweight cryptographic algorithms for constrained systems, in addition to other hardware-oriented security measures such as Physically Unclonable Functions (PUFs) and Hardware Security Modules.

This paper addresses the challenges arising from IoT device heterogeneity and the absence of standardization across vendors and manufacturers, a problem that is getting increasingly more difficult due to the short time-to-market of IoT devices and the growth of IoT devices exceeding 30 billion devices worldwide. This paper also looks at quasi-standardization attempts by integrated platforms for IoT devices and unifying software attempts present in a variety of research. This paper provides a survey across current security frameworks, highlighting both current and future research in securing the IoT ecosystem.

INTRODUCTION

Internet of Things (IoT) devices have made significant advances in how we interact with technology, improving connectivity between homes, industries, and healthcare, and creating the possibility of a truly smart city. With the global IoT ecosystem exceeding 30 billion devices and continuously growing, these interconnected systems create substantial security challenges that are vital to address for the well-being of data within industries and individuals alike. The heterogeneous nature of IoT devices, often within resource-constrained devices, creates a difficult challenge to secure devices thoroughly and in-depth.

This survey examines the current state of security across IoT devices by identifying fundamental security objectives, approaches to secure IoT devices, and attempts at standardization and reducing heterogeneity within the field. The security of IoT devices is critical as the field is rapidly expanding and handling sensitive data with larger magnitudes.

This paper's research reveals that confidentiality and integrity are primary concerns for IoT environments due to resource constraints of IoT devices, heterogeneity across manufacturers, vendors, and use cases, and the lack of standardization for security protocols in IoT. These factors create a large attack surface within networks and device types, making security in IoT difficult to maintain.

Author's address: Harry Hillsdownley.

2025. Manuscript submitted to ACM

The remainder of this paper is organized as follows: examining the fundamental security objectives of IoT systems, analyzing how current computer security implementations are being adapted to more resource constrained, energy efficient algorithms, and addressing the lack of standardization by looking at approaches to attempt to standardize the security protocols of a wide variety of IoT devices. This paper aims to look at technologies currently being implemented in the field, such as Symmetric Homomorphic Mapping, blockchain implementations, physically unclonable functions, and integrated IoT platforms that aim to unify security across diverse IoT ecosystems.

FUNDAMENTAL SECURITY OBJECTIVES

Fundamental security objectives are critical to computer security, standing on pillars such as confidentiality, integrity, authentication, privacy, availability, trust, and non-repudiation. These security objectives are essential in the context of Internet of Things (IoT) devices, which will operate in diverse environments by communicating autonomously.

IoT devices are challenging to secure due to various constraints within the device itself and the larger network of IoT devices, such as resource constraints, heterogeneity, physicality and controlled environment, and lack of standards. Hence, securing comprehensively relies on a wide variety of adaptations and approaches specific to IoT devices.

Current research in the field primarily focuses on protecting confidentiality and integrity, as the availability of IoT devices is not a vulnerable target for attacks.

To protect confidentiality, one research approach is introducing a new data aggregation algorithm for user data, to protect user privacy and avoid expensive public key encryption, which is usually not plausible due to the computational constraints of IoT devices [7]. This approach is based on using Symmetric Homomorphic Mapping (SHM), which allows for summing encrypted values without decrypting them, which then gets aggregated in the cloud due to IoT's compute constraints [7].

This approach effectively protects confidentiality and integrity by aggregating multiple encrypted datablocks from multiple IoT devices without ever decrypting them. This approach helps protect IoT devices from a Layer Adding Attack, where the attacker aggregates information to manipulate the result. The resulting data is protected from layer adding attacks as encrypted data gets aggregated, and when the Authrity Center for compute, wants to use the data with its symmetric key, the added layer will raise flags by not being able to decrypt correctly in addition to the difficulty of bypassing the binding factor linked to each data source [7].

Another approach for protecting the confidentiality and integrity of data across IoT devices is the implementation of a blockchain ledger. Blockchains are incorruptible, decentralized digital ledger that stores transactions, ensuring data robustness by ensuring that data is stored identically across all nodes in a peer-to-peer network. Blockchains ensure the integrity and trust of the business logic data in the IoT environment. This works by providing data integrity across a large number of transactional parties, ensuring decentralized trust [4]. Additionally, there are multiple levels for implementing blockchains from end to end, gateway or device level, to ensure how different data might need to be protected at different levels, given the compute constraints of IoT devices [4]. Blockchain approaches are also able to guarantee a secure chain-of-custody for various sensitive data streamed from IoT devices to their computation servers.

CHALLENGES PARTICULAR TO IOT CHARACTERISTICS

When addressing IoT devices, one important characteristic is their limited computational resources, such as energy, communication, computation, and storage, due to their limited form factor. This size constraint poses challenges [3]. When addressing the limited computational power of IoT devices, lightweight security mechanisms play a crucial role in ensuring the security of IoT devices.

Lightweight Cryptography is a branch of cryptography that specializes in designing highly computationally and energy efficient encryption algorithms, message authentication codes, and hash functions [3]. Additionally, the problem only grows due to the heterogeneity between IoT devices. Researchers have come up with standards like ISO/IEC 29192, which specify a lightweight security standard that includes block ciphers such as PRESENT and CLEIFA, hash functions such as PHOTON and SPONGENT, and other lightweight algorithm families such as SIMON and SPECK. These algorithms are designed to work on the computing resources of IoT devices.

However, despite the wide range of algorithms that are available for on-device, some common techniques to ensure fundamental security, such as authentication procedures, are pending to be developed due to the lack of standardization of a lightweight encryption algorithm that can be implemented in the hardware or supported by common cryptographic libraries [2] [3].

In addition to generating new lightweight algorithms, researchers are also focusing on adapting and improving the performance of existing algorithms and protocols for IoT [5]. A famous example of adaptation of algorithms for IoT that is mentioned by literature is that of cryptographic primitives, such as the elliptic curves, which were too complex for constrained devices such as IoT, however, once optimized for memory overhead and energy consumption, they enabled protocols such as key agreement and digital signatures to run at the smallest-compute level of IoT, the sensor level.

Researchers are also attempting to add defense in depth to IoT devices by creating secure hardware approaches [5] [3]. PUFs or (physically unclonable functions) are used to generate unique hardware fingerprints or cryptographic keys based on hardware manufacturing variations within the IoT device [5]. This approach mitigates the need for key storage and reduces the attack surface due to memory errors within the device.

ADDRESSING HETEROGENEITY AND LACK OF STANDARDS

The lack of heterogeneity and standardization for secure protocols, software, and encryption algorithms across IoT devices hinders their security by increasing the attack surface and making it difficult to develop well-established security-by-design methods. The number of interconnected IoT devices has surpassed the 30 billion device marker, making the challenge for standardization and addressing heterogeneity increasingly difficult and important [6].

The root cause lies in the lack of a unified definition of IoT, with different industries, consumers, and researchers using different definitions based on specific services/architectural approaches. This also instills the architectural challenges of reducing heterogeneity, where a lot of IoT devices are built on a three-layer or five-layer architecture. The five-layer architecture, while being the most secure, is also the longest time-to-market for these devices [1]. If standardization is achieved, the attack surface for most of the 30 billion devices would be greatly reduced [6].

Efforts are being made to mitigate the heterogeneity and lack of standardization challenges in the IoT field. Some attempts have been made to standardize the security on IoT devices by organizations such as IETF, IEEE, and ISO/IEC [5]. In addition, IoT-specific profiles for Datagram Transport Layer Security and Transport Layer Security are currently being integrated into production for constrained devices [5]. This integration for constrained devices, especially with the newly developed or repurposed encryption algorithms, seems like a promising way to secure the intercommunication between these devices. Once interconnection security is established, the attack surface is greatly reduced by protecting confidentiality.

In addition to standardization, the implementation of technical solutions is also an approach that is being used to increase security. While this is technically not standardization, a wide variety of papers mention the same systems being employed to address challenges caused by heterogeneity, such as Intrusion detection systems, Hardware-based security, platform-based solutions, and trusted gateways.

Intrusion detection systems (IDS) act as an additional line of defense by detecting unusual activity within the device itself. IDS monitors the activities of a host or network and can trigger alerts when unusual behavior is detected [6][5]. IDS's primary goal is to protect against unusual actions and safeguard the user's privacy [6]. This approach seems to be promising, however, multiple papers also outline why creating an accurate IDS is challenging. Given the resource constraints, it is hard to create a system that is accurate and reduces false alerts, which implies difficulty in assessing malicious activity to avoid disrupting normal operations [6]. As long as an effective IDS system can be developed, it could be standardized to provide a solid approach towards a software-based security protocol.

Hardware-based security for IoT devices is mainly based on Hardware Security Modules being developed. A Hardware Security Module (HSM) is a device that can be connected to an IoT device and provide a framework for authentication and integrity [6]. HSMs provide a scaffolding for efficiency and security for IoT devices by containing a good cryptographic engine, storing private and public key pairs that cannot leave the module, and offering physical tampering detection [6]. This approach aims to provide a modular approach for IoT security, which is good given the heterogeneous nature of IoT devices across manufacturers and vendors. However, this does raise the question of whether HSMs will be able to provide security to all devices despite differences in manufacturers, vendors, and software being used by the devices. If the software being used by IoT devices does get standardized, this might be a good approach to increase security without harming the device's computational ability by offloading security processes to the HSM.

An approach to overcome the lack of standardization across devices is integrated platforms, which support a wide variety of devices, environments, programming languages, and protocols with high security [5]. IoT platforms such as IoTivity and FIWARE are mentioned to extend security features such as access control, service isolation, and anonymous credentials [5]. These integrated platforms support a wide variety of IoT devices, making it a potential for standardization across the field, and provide a solid foundation for secure computing and communication within IoT devices.

FUTURE WORK

The survey above reveals that the current IoT security landscape has areas where further research could benefit the field significantly. As IoT devices expand in numbers, addressing this research to provide robust security frameworks and features to IoT becomes increasingly vital.

This paper identified primary areas for further development for the security of IoT devices, including lightweight authentication frameworks and robust and accurate intrusion detection systems.

Lightweight authentication frameworks, especially optimized for resource-constrained devices, or even standardized authentication protocols, would enable authentication without overwhelming compute resources. This is advantageous because current authentication implementations rely on private and public keys, which can be overwhelming for the system. By designing lightweight authentication frameworks, we would make a framework available across a variety of IoT devices despite their computing power. Furthermore, this research would reduce identity-based attacks across networks of IoT devices, greatly reducing the attack surface and the heterogeneity within approaches for authentication for IoT devices.

When used in combination with other existing frameworks or approaches for IoT device security, accurate and robust Intrusion Detection Systems (IDS) can provide a modular, widely compatible defense-in-depth mechanism for IoT devices. By monitoring network traffic patterns and device behaviors, an advanced IDS implementation could identify activities that bypass traditional security mechanisms, such as access control, when encryption is too computationally expensive. IDS can serve as a unifying security layer across different device types and computational power across manufacturers and security implementations, reducing the need to be standardized, but rather easily implemented.

Additionally, IDS systems could be implemented at various levels within the IoT architecture, from edge devices to cloud levels, creating a security hierarchy for data across levels, greatly reducing the attack surface without needing standardization, assuming that this system is lightweight and easily implemented into existing hardware solutions.

In conclusion, this paper believes that the two most important areas for further research to secure IoT devices across networks are lightweight authentication frameworks and intrusion detection systems, as they can greatly reduce the attack surface across various levels within the IoT architecture.

CONCLUSION

This survey has examined the current state of security across IoT devices by identifying fundamental security objectives, implementation challenges, and emerging solutions in the field. As the IoT ecosystem continues to expand beyond 30 billion interconnected devices, the security challenges become increasingly complex due to the unique characteristics of IoT environments.

The research conducted in this survey reveals that confidentiality and integrity remain primary concerns for IoT devices due to the heterogeneous nature of the field, resource constraints, which make it infeasible to use current technologies to secure IoT devices, and the lack of standardization for security protocols. These factors expand the attack surface across billions of interconnected devices, making in-depth security hard to achieve.

This survey identified various approaches being implemented to address these challenges. Symmetric Homomorphic Mapping (SHM) allows for data aggregation without decryption, blockchain implementations provide a decentralized trust mechanism, lightweight cryptography offers computationally efficient security for constrained devices, and hardware security measures provide additional layers of protection without exhausting computing resources. These approaches are novel, but still leave a large attack surface.

As shown in the future work section, lightweight authentication frameworks and robust intrusion detection systems are key areas for further research. Lightweight authentication frameworks would enable secure identity verification without overwhelming the computational resources of IoT devices. Additionally, advanced IDS implementations could provide defense mechanisms that identify malicious activities across different device types and implementation levels.

In conclusion, while significant progress has been made in addressing IoT security challenges, the rapidly evolving nature of IoT technology requires innovation and adaptation of security protocols. By focusing on the development of lightweight, standardized security protocols, hardware-based security solutions, and accurate intrusion detection systems, the IoT ecosystem can be more secure, despite the computational constraints and heterogeneity in this field.

REFERENCES

[1] Al-Qaseemi, S., Almulhim, H., Almulhim, M., and Chaudhry, S. Iot architecture challenges and issues: Lack of standardization. pp. 731–738.

[2] Alshahwan, F. *Adaptive Security Framework in Internet of Things (IoT) for Providing Mobile Cloud Computing.* 05 2018.

[3] Meneghello, F., Calore, M., Zucchetto, D., Polese, M., and Zanella, A. Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices. *IEEE Internet of Things Journal PP* (08 2019), 1–1.

[4] Minoli, D., and Occhiogrosso, B. Blockchain mechanisms for iot security. *Internet of Things 1-2* (2018), 1–13.

[5] Roman, R., Lopez, J., and Gritzalis, S. Evolution and trends in iot security. *Computer 51* (07 2018), 16–25.

[6] Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., and Stiller, B. Landscape of iot security. *Computer Science Review 44* (05 2022).

[7] Zhou, J., Cao, Z., Dong, X., and Vasilakos, A. Security and privacy for cloud-based iot: Challenges. *IEEE Communications Magazine 55* (01 2017), 26–33.