ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

IOT Security and Privacy Using Encryption Algorithms

Dr. Rajendra Kumar Bharti

Associate Professor, Computer Science & Engineering, Bipin Tripathi Kumaon Institute of Technology, Dwarahat, Uttarakhand, India

ABSTRACT: The increasing adoption of the Internet of Things (IoT) technology has brought an increase in security challenges. Given the limited processing power of most IoT devices, encryption seems to be a plausible method for ensuring data protection. This article explores how encryption helps, along with its algorithm types. The concept of the Internet of Things (IoT) is slowly finding applicability across various industry verticals, resulting in a higher business value. IoT transforms process monitoring by connecting and tracking multiple devices within a network.However, beyond the benefits of IoT lies a great challenge of ensuring security throughout the communication network. The threat is evident through the numerous incidents of illegal data manipulation and hacking devices on the network, such as cameras and vehicles.IoT-connected gadgets have a bad reputation for poor security partly because they are often made cheaply and in haste and partly because they lack computing power. Conventionally speaking, it is not so easy to encrypt all that data with limited resources.However, real-world data suggests that these tiny IoT gadgets and IoT sensors can run independent versions of traditional, time-tested encryption schemes. What is encryption, you ask. It is the process of encoding information or converting the original information into an alternative, also known as ciphertext. More on that in a bit.

KEYWORDS: encryption, algorithms, IoT, security, privacy, data protection, hacking devices, resources, ciphertext, bit

I. INTRODUCTION

The biggest security-related threat of IoT systems is that even using devices for data collection from the real physical world can become a target of cybercrimes.For example, deploying the IoT technology to a plant can significantly enhance productivity and maintainability via data collection from many sensors and modules installed in the production equipment.Falsifying sensor data during the process can result in incorrect analysis and erroneous control. Even if there are no problems, it is important to consider risks and threats that might become evident or pronounced in the future. IoT is now subject to encryption regulations, and the technology must be applied to all devices within restricted environments. These regulations include various types of algorithms - simply known as IoT encryption algorithms.[1]

These security tools protect IoT devices and networks from potential data breaches and communication vulnerabilities. So, how does encryption work? The original information, known as unencrypted data or plaintext, undergoes a simple process of translation known as encryption.Under the process, the plaintext or original information translates into a secret code, which appears to be a useless set of random characters known as encrypted data or ciphertext. On the other hand, decryption translates the secret code to the original information through a process known as cryptanalysis.[2]The science of applying end-to-end encryption and decryption is known as cryptography, and the study of cryptography and cryptanalysis is known as cryptology. It includes various mathematical theories, formulas, and algorithms known as ciphers, also quoted as encryption or cryptographic algorithms. The ciphers use variables known as keys or cryptographic keys to lock and unlock encryption or decryption functions[3]. Users create a secret security code known as the password to generate keys. These operate on two types of encryption:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

1. Symmetric - A secret key encryption

As the name defines, it uses the same single key to function encryption and decryption. In this case, it is a must that the sender and receiver agree on the shared secret key before establishing the secured communication.Depending upon the data exchange requirement, symmetric encryption operates on stream (1 byte or 1 bit) and block ciphers (data of fixed size - usually 64 bits). It is faster, requires low power, and includes a simple, straight forward end-to-end process. AES, DES, IDEA, and Blowfish are examples.[4]

2. Asymmetric - A public key encryption

Unlike Symmetric Encryption, it uses a key pair - a public key for encryption and a private key for decryption, linked mathematically and logically to each other.Any sender can encrypt the data using the public key. However, the decryption is only possible by the intended recipient using the private key. Thus, asymmetric encryption involves authentication with strengthened security. The top examples are RSA, DSA, ECC, and TLS/SSL.Since IoT architecture works on the heterogeneous distributed system, it uses the symmetric type for encryption and the asymmetric type for decryption to cope with the security challenges.The fundamental security concerns of an IoT ecosystem are access control, privacy, and robust user authentication. [5]

The best encryption algorithms for IoT are:

1. The Data Encryption Standard (DES) and Triple-DES

Both are the symmetric encryption algorithms wherein DES is the oldest and keystone of the cryptography, now phased out (due to low encryption key). Triple-DES is its successor, believed to be effective till 2030.The Triple-DES overcomes all DES challenges, such as vulnerable meet-in-the-middle attacks, applies three 56-bit keys to every data block, and adds the total key length up to 168-bit.[6]

However, there is the case of a mid-level vulnerability that depreciates its security level to a 112-bit key. Due to this, it is phasing out (replaced by AES). But some IoT products and financial services still utilize it because of its dependability, compatibility, and flexibility.[7]

2. Elliptical Curve Cryptography (ECC)

It is an alternative to Rivest–Shamir–Adleman (RSA) and utilizes algebraic functions to create concrete security between “key pairs” (public and private keys).Deploying the elliptic curve theory, ECC generates shorter, faster, and more efficient keys for encryption and decryption. That makes it the best fit for IoT devices, mobile applications, and those with limited computing (CPU) resources.[8]

3. Advanced Encryption Standard (AES)

It is the most popular and robust symmetric encryption algorithm, which works on block ciphers from basic 128 to heavy-duty 192 and 256-bit keys. It is unbreakable (due to longer key length) and immune to cyber-attacks except for brute force.As a result, the US gogovernment'sSA, NIST (developer of AES), and other large organizations extensively use AES to safeguard classified sensitive data. Also, it is the futuristic “best-fit standard application” for the private sector.[9]

4. Digital Signature Algorithm (DSA)

Like RSA, it is also an asymmetrical encryption algorithm with a slight yet significant difference in the process. DSA uses an electronic/digital signature for data transmission, which makes encryption slower (as it involves authentication).However, decryption is faster after the successful verification (through hash function). This operation

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

uses the mathematical concept of modular exponentiation and the algebraic properties of the discrete logarithm. Lightweight Digital Signature Based Security Algorithms are in research to establish secure communication in an IoT ecosystem.[10]

5. Rivest–Shamir–Adleman (RSA)

It is a scalable asymmetrical encryption algorithm and is most trusted for the data in transit over the internet like SSL/TLS, S/MIME, SSH, cryptocurrencies, etc.It efficiently defends against brute-force cryptographic hacks by using higher key lengths (768, 1024, 2048, 4096-bits, and more), which makes it difficult and time-consuming to decrypt the data. Hence, the go-to for IoT applications.[11]

6. Blowfish and Twofish

Both are the leading license-free, public domain symmetric encryption algorithms wherein Twofish is the successor of Blowfish. Blowfish deciphers plain text into 64-bit data blocks and Twofish into 128-bits (in 16 rounds irrespective of key size). The high speed plus flexibility make them unbreakable and user-friendly.

Consequently, Blowfish is most suitable for securing e-commerce applications, online payments, and passwords. Twofish is an excellent choice for hardware and software solutions, extensively used for low processing resources.[12]

II. DISCUSSION

Businesses that have invested heavily in the traditional perimeter IT security firewalls and detection solutions want more vital data protection. From external hackers to internal staff, data protection for different formats and purposes is a humongous task. Encryption takes care of the following tasks:

1. It supports the set regulations and compliances under Payment Card Industry Data Security Standard (PCI DSS) and other market advanced encryption standards. That aims to protect the sensitive data of cardholders during online transactions.[13]

2. It holistically safeguards confidentiality, authentication, integrity, and data privacy irrespective of location (cloud/local storage). It helps promote trust and enhances security at all times.

3. It is platform-independent and protects data at rest, in use and in motion, across various IoT devices, eventually strengthening the network communication.

Amidst the rising IoT data security vulnerabilities, solid and undefeatable encryption is necessary. However, it comes with a few disadvantages:

1. The top problem is encryption key management at an enterprise level. Its maintenance is a colossal task, and if not deciphered with the corresponding private key, it does not give access to anyone. It may restrict access even for the data owners. The arrangement implies that all the associated data will get lost if you lose the encryption keys.

2. It includes considerably high expense in maintaining and upgrading the systems and backup servers that perform data security tasks. In addition, the recovery operation in a large-scale disaster consumes a lot of time.[14]

3. The encryption backup and restoration process is complex and sometimes faces compatibility issues while integrating with IoT applications. This, in turn, adversely impacts the daily routine operations.Therefore, data encryption needs a concrete strategy to backup the keys separately. It must be secure from cyber attackers and intruders but easily accessible for the data owners.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Conventional cryptography is unsuitable for IoT technology as it requires low-power computation resources. Although AES, SHA-256, and RSA/DSA/Elliptic Curve perform well together. However, they mostly struggle with IoT and embedded ecosystems.That is why lightweight cryptography (LWC) is the best solution to deal with the next generation of IoT frameworks based on emerging 5G technology and Industry 4.0.LWC is still at a nascent phase and has been found incredibly compelling for the small size, low-energy IoT products such as RFID tags, sensor networks, microcontrollers, contactless smart cards, smart watches, and so on.PRESENT, CLEFIA, PICCOLO, PRINCE, and LBLOCK are the prominent lightweight cryptographic algorithms currently used in IoT applications in a testing environment.Cyber experts are constantly optimizing the existing cryptographic standards and devising new algorithms to secure data transportation and communication channels.[15]

Errors in data encryption cost businesses a lot. Major data breaches lead to huge losses in brand reputation and monetary solutions. These errors originate due to sheer negligence and lack of knowledge. According to the World Economic Forum," 5% of cybersecurity infringements arise because of human errors. It is an enormous figure, and large-scale enterprises cannot afford to ignore it. There are fundamentally two broad categories of human errors:

1. Skill-based errors due to slips and lapses occur because of fatigue or negligence while performing daily routine operations.

2. Decision-based errors occur due to the wrong choices due to a lack of knowledge.

The top six examples of human errors in end-to-end encryption are as follows:

1) Using poor and weak passwords
2) Getting trapped in phishing and social engineering
3) Mishandling high privilege sensitive data or accounts
4) Using outdated or unauthorized software in the official system
5) Using third-party platforms to share confidential corporate data
6) Misdelivery, especially in the case of email or online workspace communications[16]

III. RESULTS

All of the above are resolvable with the below-mentioned six precautionary solutions

1) Incorporate corporate security policy and organize regular cybersecurity training
2) Perform regular IT audits
3) Enforce Zero Trust Security Policy with the least privileges
4) Opt for cloud storage management for easy data retrieval and restoration
5) Enable two-factor authentication to strengthen sensitive data/admin security
6) Block all third-party tools, USB devices, and applications to prevent cyberattacks[17]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

The future of IoT security

The expansion of IoT technology across industries has boosted the growth of a 360-degree security market. Though it has slow adoption, potential growth is evident thanks to the ongoing rapid technological developments, such as smart homes, 5G, and automotive.

The future of IoT security

We will not be surprised to see IoT attracting full-stack protection services in the upcoming years. The future of IoT security is likely to be dependent on the below practices:

1. Threat intelligence and security updates

By 2025, the number of IoT connections per minute will be 1,52,200, producing approximately 73.1ZB of data. With such enormous data transmission, IoT devices should regularly receive security patches, including threat intelligence, to combat infringement risks.[18]

2. Layered security approach

Since the IoT ecosystem is a network of heterogeneous devices, deploying multiple security layers at each data exchange point will be necessary.

3. Constant data monitoring

Amidst the 24*7 data exchange, IoT will help discover, monitor, manage, and analyze the overall dynamic systems, including billions of events and alerts. IoT monitoring will significantly defend the “inter and intra”-connected applications, including GPS signals. [19]

4. Hardware firewalls

The IoT firewalls that are device and application-centric are known as hardware firewalls. Their core operation is to ensure protection from phishing scams, unauthorized remote access, and suspicious network traffic.

5. Backup integration

Cloud backup integration solutions will be the most suitable to handle and secure the edge computational-based IoT framework, including devices, networks, and data. Furthermore, network segmentation would be an added advantage to stop the attack's spread and isolate the infected machines.[20]

Consumers also have a role to play in IoT security.

How can end-users find secure IoT devices? No one has to be an expert in data encryption to secure their internet-connected devices appropriately. IoT home and business security start with the network router.Similarly, any new IoT device introduced to the system will have security settings by default, including resetting any default passwords for gaining network access and two-factor authentication (2FA) to keep software patches up to date.The consumer IoT market is growing exponentially year over year and is predicted to reach $142 billion at a CAGR of 17.52% by 2026. Therefore, with the increasing popularity of this next-generation technology, it is equally important to educate consumers about the five IoT security essentials:

1) Changing the universal default password

2) Enabling two-factor authorization or 2FA

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

3) Updating the IoT devices with the latest software version

4) Communicating on an end-to-end secure network like password-protected Wi-Fi

5) Securing the personal data in a separate cloud-based storage system[21]

IoT is already revolutionizing both the lifestyle and professional aspects of consumers. The scope of IoT is ubiquitous, from home automation to wearable technologies and industrial applications. Undoubtedly, it is making life much easier.However, the increasing security challenges need special attention to prevent cybersecurity breaches on a disastrous level. Hence, in support of the existing Blockchain encryption algorithms, it is time to devise new defense mechanisms and standardize proposed lightweight cryptographic options to keep pace with the progressing IoT applications.[22]

IV. CONCLUSIONS

The way IoT has transformed our lives - at both consumer and industrial levels - is fascinating! The technology has spread from home smart fridges to factory production line tracking. Therefore, the devices that connect to the internet must be encrypted because of the nature of data transmitted.IoT users and security managers can minimize data breaches to a great extent and ensure a seamless experience through encrypted IoT networks and devices. [23]

REFERENCES

[1] IPv6 http://www.rfc-editor.org/rfc/rfc2460.txt
[2] VaultIC http://www.insidesecure.com/Products/ Embedded-Secure-Element
[3] Sony RND compromise http://www.exophase.com/20540/hackersdescribe-ps3-security-as-epic-fail-gainunrestricted-access/
[4] PKCS#11 http://www.emc.com/emc-plus/rsalabs/standards-initiatives/pkcs-11- cryptographic-token-interface-standard. htm
[5] CMP http://tools.ietf.org/html/rfc4210
[6] MatrixSSL http://www.peersec.com/matrixssl.html
[7] OpenSSL Heartbleed http://info.insidesecure.com/heartbleed
[8] QuickSec IPSec http://www.insidesecure.com/Products/ Protocol-Security-Toolkits/QuickSecIPsec-Client-Toolkit
[9] Minimal IPsec and IKE – IETF http://tools.ietf.org/html/draft-kivinenipsecme-ikev2-minimal-01
[10] Geovandro C. C. F. Pereira, Renan C. A. Alves 2017.Performance Evaluation of Cryptographic Algorithms over IoT Platforms and Operating Systems, Security and Privacy in Emerging Wireless Networks, Hindawi.
[11] Jurcut, Anca & Ranaweera, Pasika & Xu, Lina. (2019). Introduction to IoT Security. 10.1002/9781119527978.ch2.
[12]. Kumar, S., Tiwari, P. & Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data 6, 111 (2019).
[13]. Mohammed, Husamuddin & Qayyum, Mohammed. (2017). Internet of Things :A Study on Security and Privacy Threats. 10.1109/Anti-Cybercrime.2017.7905270.
[14]. Muthuswamy, Sujithra & Ganapathi, Padmavathi. (2016). IOT Security Challenges and Issues – An Overview. 6. Monshizadeh, Mehrnoosh & Khatri, Vikramajeet. (2018). IoT Security. 10.1002/9781119293071.ch11.
[15]. Perwej, Dr. Yusuf & Parwej, Dr. Firoj & M., Mumdouh & Akhtar, Nikhat. (2019). The Internet-of-Things (IoT) Security : A Technological Perspective and Review. Volume 5. Page 462-482. 10.32628/CSEIT195193.
[16]. Shaikh, Eman & Mohiuddin, Iman & Manzoor, Ayisha. (2019). Internet of Things (IoT): Security and Privacy Threats. 1-6. 10.1109/CAIS.2019.8769539.
[17]. M, Sheik dawood. (2018). Review on Applications of Internet of Things (IoT).
[18].Sufian Hameed, Faraz Idris Khan & Bilal Hameed (2019): Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review, Journal of Computer Networks and Communications.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

[19].Suo, Hui & Wan, Jiafu & Zou, Caifeng & Liu, Jianqi. (2012). Security in the Internet of Things: A Review. Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012.

[20] Cracking, D, "Secrets of Encryption Research," Wiretap Politics, and Chip Design, Electronic Frontier Foundation, 1998.

[21] CzeslawKoscielny, "A new approach to the Elgamal Encryption Scheme, Academy of Management of Legnica, Faculty of Computer Science, ul. Reymonta 21, 59–220 Legnica, Poland," Int. J. Appl. Math. Comput. Sci, vol. 14(2): 265-268, 2004.

[22] Daemen, J, "Cipher and Hash Function Design Strategies Based on Linear and Differential Cryptanalysis," PhD thesis, Doctoral Dissertation, KU Leuven. 1995

[23] S.Vishnupriya, "Edge Computing Based IoT for Smart Cities," SSRG International Journal of Computer Science and Engineering, vol. 7, no. 1, pp. 16-21, 2020. Crossref, https://doi.org/10.14445/23488387/IJCSE-V7I1P104