IMPACT OF INTERNET OF THINGS (IOT) ON CLOUD CRYPTOGRAPHY USING ENCRYPTION, DECRYPTION, PLAINTEXT AND CYPHERTEXT

Devendra Singh Mohan*[1], Mohit Kumar[2], Kuldeep Chauhan[3]

[1]PG (M.Tech) Scholor, Dept. of Computer Science & Engg, Shobhit University, Gangoh, India.

[2]Asst. Prof., Dewan VS Group of Institutions, Meerut, India

[3]Asst. Prof., Dept. of Computer Science & Engg, Shobhit University, Gangoh, India.

ABSTARCT

Internet of Things (IOT) refers to a network connected by smart devices (Contain Sensors) and having ability to communicate or exchange the information to each other. Cloud cryptography is based on encryption, in which computers and algorithms are utilized to scramble text into ciphertext. This ciphertext can then be converted into plaintext through an encryption key, by decoding it with a series of bits.

Keywords: IOT (Internet of Things), Cryptography, Cloud Cryptography, Encryption, Decryption, Plain Text, Cypher Text.

1. INTRODUCTION

The **Internet of things** (**IoT**) describes physical objects (or groups of such objects) with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks.The field has evolved due to the convergence of multiple technologies, including ubiquitous computing, commodity sensors, increasingly powerful embedded systems, and machine learning.Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), independently and collectively enable the Internet of things. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", including devices and appliances (such as lighting fixtures, thermostats,home security systems and cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smartphones and smart speakers. IoT is also used in healthcare systems [1].

Building upon a complex network connecting billions of devices and humans into a multitechnology, multi-protocol and multi-platform infrastructure, the internet of things (IOT) main vision is to create an intelligent world where the physical, the digital and the virtual are converging to create small environments that provide more intelligence to the energy, health, transport, cities, industry, building and other areas of our daily life. The Expectation is that of interconnecting millions of islands of smart networks enabling access to the information not only “anytime” and “anywhere” but also using “anything” and “anyone” idealy through any “path” , “network” and “any service”. This will be outfitted with sensing , identification and positioning devices and endoed with an IP address to become smart objects capable for communicating with not only other smart objects but also with humans with the expectation of reaching areas that we could never reach without the advances made in the sensing , identification and positioning technologies [2].

*Corresponding Author

In device layer lie devices (Sensors, actuators, RFIDdevices) and gateways used to collect the sensor reading for further processing while the network layer the neccessary transport and networking capabilities for routing the IOTdata processing places. The support layer is a middleware layer that serves to hide the complexity of the lower layers to the application layer and provide specific and generic services such as storage in defferent forms (database management sytem / cloud computing systems) and may other services such as translation [2].

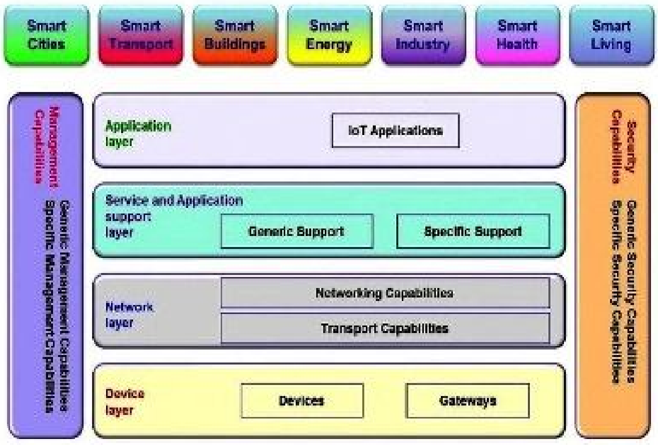


Fig 1: IOT Layered Architecture

The IOT system and application are designed to provide security, privacy, safety, integrity, trust, dependability, transparency, anonymity and are bound by ethics constraints

Advantages [5]:

- It can assist in the smarter control of homes and cities via mobile phones. It enhances security and offers personal protection.
- By automating activities, it saves us a lot of time.
- Information is easily accessible, even if we are far away from our actual location, and it is updated frequently in real time.
- Electric Devices are directly connected and communicate with a controller computer, such as a cell phone, resulting in efficient electricity use. As a result, there will be no unnecessary use of electricity equipment.
- Personal assistance can be provided by IoT apps, which can alert you to your regular plans.
- It is useful for safety because it senses any potential danger and warns users. For example, GM OnStar, is a integrated device that system which identifies a car crash or accident on road. It immediately makes a call if an accident or crash is found.
- It minimizes human effort because IoT devices connect and communicate with one another and perform a variety of tasks without the need for human intervention.
- Patient care can be performed more effectively in real time without the need for a doctor’s visit. It gives them the ability to make choices as well as provide evidence-based care.

- Asset tracking, traffic or transportation tracking, inventory control, delivery, surveillance, individual order tracking, and customer management can all be made more cost-effective with the right tracking system.

Disadvantages [5]:

- Hackers may gain access to the system and steal personal information. Since we add so many devices to the internet, there is a risk that our information as it can be misused.
- They rely heavily on the internet and are unable to function effectively without it.
- With complexity of systems, there are many ways for them to fail.
- We lose control of our lives—our lives will be fully controlled and reliant on technology.
- Overuse of the Internet and technology makes people unintelligent because they rely on smart devices instead of doing physical work, causing them to become lazy.
- Unskilled workers are at a high risk of losing their jobs, which could lead to unemployment. Smart surveillance cameras, robots, smart ironing systems, smart washing machines, and other facilities are replacing security guards, maids, ironmen, and dry-cleaning services etc.
- It is very difficult to plan, build, manage, and enable a broad technology to IoT framework.

2. CLOUD CRYPTOGRAPHY

According to privacy experts, cryptography is the cornerstone of security. Cloud cryptography is the encryption of data stored in the cloud which adds a strong layer of protection and avoids a data breach. This practice safeguards data without delaying the data delivery. Cryptography expert Ralph Spencer Power said “information in motion and information at rest can be better protected by cryptography. Virtual data needs to be stored cryptographically by maintaining the control of the cryptographic key.” Now, let us learn how to implement cryptography in the cloud and protect our cloud data. [4]

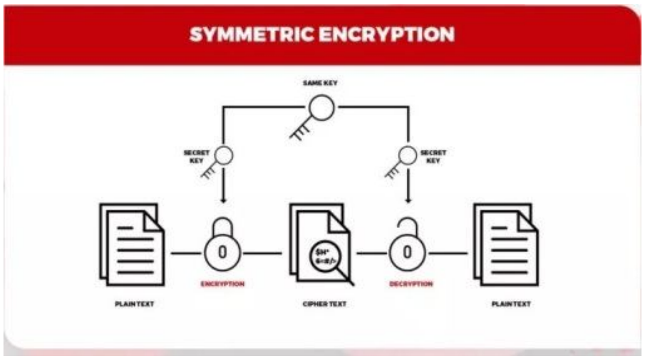
It’s not possible to control cloud data physically. Cloud encryption is a way of protecting data and communication with the help of codes. Cloud data encryption can guard sensitive data and verify asset transfer without delaying the information transmission. [4]

There are different kinds of cryptographic keys used by companies for cloud security. Cloud data encryption depends on three algorithms:

2.1 Symmetric-key
2.2 Asymmetric key
2.3 Hashing

2.1 Symmetric Algorithm

It utilizes one key for both encryption and information decoding. It doesn’t need a lot of computational power and works extremely high in encryption. Symmetrical algorithms consist of two-way keys to guarantee verification and approval. Except if the client has the key, the encoded information is put away in the Cloud, and can’t be decoded.



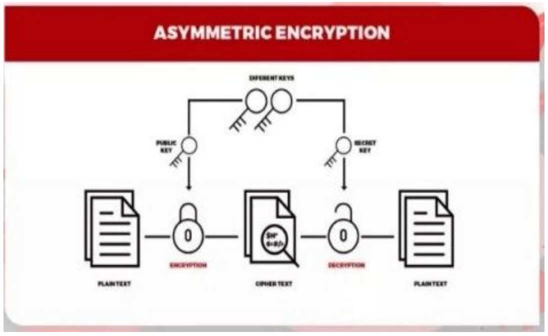
Some popular symmetric algorithms used in cloud computing algorithms are

a. **Advanced Encryption Standard (AES)** – It is used to encrypt digital data such as telecommunications, financial, and government. In AES, the same key is used for both encryption and decryption. It is a block of ciphertext that repeats itself after every defined step multiple times. It has a 128-bit block size, with key sizes of 128, 192, and 256 bits. It's efficient in both software and hardware.

Data Encryption Standard (DES) – It adopts a 64-bit secret key, out of which 56 bits are created randomly and the remaining 8 bits are used for error detection. DES is implemented in hardware and is basically used for single-user encryption, for eg – files stored on a hard disk in encrypted form.

2.2 Asymmetric Algorithm

It utilizes different keys for encryption and decoding. Here, every beneficiary requires a decoding key. This key is referred to as the recipient's private key. Here, the encryption key belongs to a particular individual or entity. This sort of algorithm is considered the most secure as it requires both keys to get to a piece of explicit data.

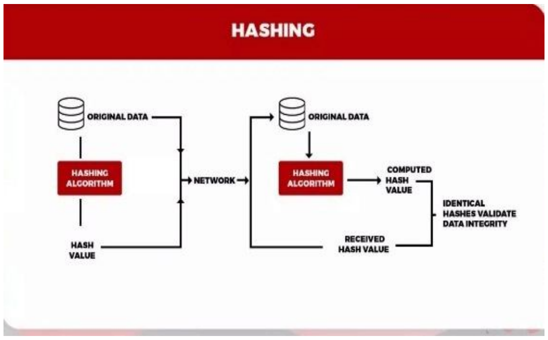


Rivest Shamir Adleman Algorithm (RSA) – It is one of the de-facto encryption standards and is used for a variety of platforms. It used different keys for encryption and decryption. The public key is known to everyone which can be decrypted using the private key only by the authorized person.

Elliptic Curve Cryptography (ECC) – ECC is modern public-key cryptography that depends on number theory and mathematical elliptic curves to generate a short key. ECC is preferred by the security experts because of the small key size of the ECC.

2.3 Hashing

It is one of the major parts of blockchain security. In the blockchain, data is put away in blocks and interconnected with cryptographic standards like a string or chain. When an information block is added to the chain, a particular code or hash is assigned to the particular block. Hashing is basically utilized for ordering and recovering things in a data set. It likewise utilizes two distinctive keys for encrypting and decoding a message. It likewise gives quicker information retrieval.



Advantages of cloud cryptography

- Cryptography in the cloud is probably the most secure strategy to store and move the information as it complies with the limitations forced by associations like FIPS, FISMA, HIPAA, or PCI/DSS.
- The information stays private to the clients. cryptography in the cloud lessens the cybercrime cases.
- Companies get warnings promptly if an unauthorized individual attempts to access the data. The clients who have cryptographic keys are only allowed data admittance.
- The encryption keeps the information from being vulnerable when the information is being transferred from one PC then onto the next,
- Cloud encryption prepares organizations to stay proactive with all due respect against cyberattacks

Receivers of the data can recognize if the information got is adulterated, allowing a prompt reaction and answer for the assault.

Disadvantages of cloud cryptography

- Cloud cryptography just grants restricted security to the information which is in transit.
- Cloud encryption needs exceptionally advanced systems to maintain encrypted information.
- The frameworks should be adequately versatile to update which adds to the involved costs.

3. CONCLUSION

Impact of Internet of Things (IOT) on Cloud Cryptography Using Using Encryption, Decryption, Plaintext and Cyphertext is a new topic for the researcher in Network security for the transmission of data from one place to another in cloud envirnment.

REFERENCES

[1] https://en.wikipedia.org/wiki/Internet_of_things

[2] (Antonio Linan Colina,Alvaro Vives, Macro Zennaro, Antoine Bagula, Ermanno Pietrosemoli) “Internet of Things in Five Days” page 15.

[3] https://archive.org/details/IoT5days/page/n14/mode/1up?view=theater

[4] https://peoplactive.com/cryptography-in-cloud-computing/

[5] https://www.geeksforgeeks.org/advantages-and-disadvantages-of-iot/

[6] Springer “Understanding Cryptography