A Lightweight Digital Signature Generation Mechanism for Authentication of IoT Devices

K. Sambasiva Rao, M. Kameswara Rao

Abstract: Internet of Things (IoT) is a rising technology which is several devices is connected through the Internet. The devices communicate with each other over the network and produce a new reality to us. In order to enjoy this new environment, the security of the devices is much essential. The lightweight cryptography is superior to the conventional cryptography. In hardware implementations, chip size and energy consumption are less compared to the general cryptography. In software implementations, the smaller code and RAM size are preferable for lightweight applications. The primitives of the lightweight cryptography are encryption, hash functions, and digital signature. The sensor data is encrypted by using hash functions and digital- signature. In this project, we are using the above methodologies analyzing the security in IoT.

***Index Terms*: IoT, Encryption, Hash Functions, Digital signature and Light weight cryptography.**

I. INTRODUCTION

The internet of things (IoT) is greatly applied in an every-day life application such as healthcare systems, smart homes, and security systems. The iot is growing rapidly day by day. Lots of devices are connected to the internet. [13]The iot devices sensing a large amount of physical environment data and condition of an object, most of the iot devices have limited storage capacity. So sensing data need to be stored at a resource-rich platform such as cloud .on the other side previously stored data is compulsory for decision making of various iot applications. For example, smart health care systems the system monitors the conditions of patient health and compare with previously stored data from the cloud for an analyzing and decision making purpose.

IoT devices are usually insulant in terms of security, either due to lax producing standards or as a result of devices don't have the process high power or space for storing to be secured. Moreover, whether or not one device is correctly secured, unsecured devices will still exist within the organization’s system entirely bypassing the scope and reach of IT security groups. Architecturally-based IoT threat modeling will reveal these IT security bypasses.

Without specific IoT security, the iniquitousness and generality of the organization’s IoT system mean organizations will simply lose management of their attack Surface. Organizations will, for instance, dictate and enforce policies that no personal sensible devices are brought into the work setting. All that care and observation is thrown out the window if one worker logs into the IT system whereas functioning from home. Whereas it's doable to stop workers from delivery sensible devices into the work setting, it might be troublesome to manage guests with IoT devices from getting into the building. Securing the IoT system merely can't be done by policy mandates. Cryptography is an art of security technique wherever messages are encoded during a non-readable type. [3] In straightforward words, it's nothing however a method employed in the protection of information throughout the transmission from sender to receiver and unauthorized access is denied. Therefore, security and confidentiality are much needed during this side. The main focus and discussion during this paper would get on numerous techniques of “Lightweight Cryptography (LWC)” and analyzing which might be the simplest methodology.

The design of an iot data integrity involving three key aspects: sensing devices, data application, and cloud. In IoT, sensing data are two types one is continuous data and event-based data. The device which is capturing continuously with certain time intervals is continuous data. And the other one is data stored when the event is detected.

At the same time, data controlling is an important section. The devices have limited data storage so some of the data storage servers such as cloud make an important role in the IoT. While using third-party cloud servers must be a focus on the security. The uploaded data in the cloud is used for prediction and analysis purpose. If hackers and third-party members have altered the data in the cloud make the wrong decisions and cause economically and human life losses.so the authenticity and integrity which assure the data from the sensing devices and not been altered or corrupted these are important for the iot applications. Without these, iot applications may take wrong decisions and false analysis.

Up to now, there is no perfect solution to find these challenges. Since the sensing devices and data applications cannot communicate directly in sessions, and transport protocol can't be used. The digital signature is a way to make sure that electronic document like text, spreadsheet, etc., authenticates. Authenticate define that sender creates the document and does not been altered of any cases since the sender creates it.

Digital signature produces on a particular type of encryption to make sure authentication. [13]Encryption is an operation which collects all types of data from one system is transferring the data to another system that will be only able to decrypt it. Authentication is a procedure to confirm that data is coming from the desired source. [14]

Revised Manuscript Received on 30 March 2019.
* Correspondence Author

K.Sambasiva rao*, Department of ECM, Koneru Lakshmaiah Educational Foundation, Vijayawda, India.
M.Kameswara rao, associate professor Department of ECM, Koneru Lakshmaiah Educational Foundation, Vijayawada, India.

The digital signature provides to secure data authenticity and integrity. The mechanism is the sender's message m is hashed the hashing algorithm h .the hashed data is called a message digest. The message digest combined with the sender's private key k to encrypt the data by that key. The data is stored in a document which is digitally signed by a signer by using the sender's private key.

[15]The digitally signed document is verified by the receiver using the same hash algorithm which is used by the sender side and decrypted by the senders public key if both are valid successfully the original message can't be altered.

II. RELATED WORK

Lightweight cryptography optimizing algorithms are mostly used in constrained environments. Andrey Bogdan et al., have proposed 13 SPONGENT variants for various levels of collision and preimage resistance and implementation constraints. They provide several ASIC hardware implementations ranging from lowest to highest areas. They also proved different essential properties of SPONGENT permutations and also given a security analysis in terms of pre image resistance and collisions. [1]

Hummingbird algorithm is one of the lightweight cryptographic algorithms appropriately used in resource-constrained environments. Xunjun Chen et al., have presented that shortcut attack on the internal 16-bit block length, and 64-bit key block cipher. Their results have shown that hummingbird-I may not achieve the security goal with its design choices. [2]

IoT which deals with many small numbers of devices and a large amount of data. The devices can interact with other devices through a global wired/wireless network to the internet. So a large amount of data impacts the security and privacy of the connected devices. Jun-Ya Lee et al., have proposed an encryption method based on XOR manipulation instead of complex encryption such as using the hash function, for privacy protection and anti-counterfeiting. [3]

Security is the main pillar for the success of IoT based services. The things which are connected in IoT are resource constrained devices with limited processing and storage capabilities. So, lightweight, is an efficient way of providing secured communication in the IoT are needed. Oriol Piñol et al., have presented lightweight implementation and evaluation of ECC for the Contiki OS. ECC is the first lightweight BSD-licensed ECC for the IoT devices are feasible of implementations by a through performance analysis using several implementations and optimization algorithms. [4]

IoT finds an enormous application in the field of an information management system, agriculture, predicting the natural disaster, healthcare monitoring, D.Jamuna Rani et al., have presented various encryption lightweight techniques and also improving the performance, security, cost of analyzed of IoT applications. [5]

Manish Kumar et al., proposed encryption model would enable a range of IoT devices to share the data with other devices or humans more securely over an insecure communication channel and also need to provide enhanced data integrity. The implemented model keeps the size of the output chipertext unchanged by XORing the parity bits to avoid overhead and making it lightweight. It denotes that the model could be used for IoT devices and systems are more difficulty to protect data. [6]

IoT based home automation systems are connected with various objects and many home appliances in a single logical network. Due to connecting of various devices data transmission among different devices within the single network or without human interventions security vulnerabilities issues will take place. Sanaah Al-Salami et al., have addressed some issues, smart homes devices contain can contain crucial information related to user's privacy and safety. They proposed a lightweight encryption scheme by using flexible public key management through adopting identity-based encryption and also provided some security analysis through simulation techniques. [7]

Due to the ubiquitous nature of the sensors increases the sensitivity of user data, so security of IoT is the most concern in these days. Sriram Sankaran et al., have proposed a lightweight security framework for IoT using identity-based cryptography and also developed hierarchical security architecture for IoT and developing protocols for secure communication. They provided simulations based results using Contiki and RELIC and shown that the proposed protocols should be efficient. [8]

Security plays a prominent role in IoT network to prevent the misuses of data, modification of data, unauthorized access of data, data monitoring etc. In IoT architecture from the bottom label to top label needs security. Effy Raja Naru et al. said that if IoT cannot protect the data from attacks, hackers and vulnerabilities then that technology should not be efficient. For implementing security in IoT lightweight protocols should be needed. So for encryption of data, classical cryptographic algorithms are used because the IoT devices are resource constrained. They have presented how to secure the IoT data transmission by using various lightweight protocols. [9]

Vijay Dahiphale et al., have presented a lightweight algorithm based on cipher i.e., ANU-II compared to previous algorithms it is most effective and efficient. ANU II needs only 24mW of dynamic power for cipher design. ANU II consists of single S-Box few shift operators and a couple of XOR gates. It is the smallest lightweight design in terms of execution time, power consumption and memory requirement. [10]

Providing security for IoT is one of the major concerns, one of the best approaches for providing security is ECC with high computational efficiency and less energy consumption. Kinza Sarwar et al., have proposed a lightweight ECC watermark scheme to overcome the ECC based schemes limitation using fragile zero watermarking technique instead of a digital signature for authentication. [11]

IoT application is becoming important in day to day lifestyle such as healthcare, smart grid, smart home, smart parking. Introducing IoT to the healthcare applications fetch several benefits, including health care provider costs, transportation costs, cost savings through lowered hospital visiting costs, insurance costs, and human resource costs. It leads to an added advantage of improved quality care in the health care domain. Depending on the rapid development of

E-health care applications which is based on IoT for providing security and privacy of the data should be the major concern like authentication of the different connected entities, energy efficiency and exchanged data confidentiality form the major concerns for users. To develop a lightweight secure authentication model, which offers significant security level against multiple attacks such as mainly: Impersonation attacks, a man in the middle attack and unknown key sharing attacks for IoT base E-health domain. Maria Almulhim et al, have proposed a secure group-based lightweight authentication scheme for IoT based E-health applications, the proposed model will provide mutual authentication and energy efficient, and computation for healthcare IoT based applications. [12]

III. PROPOSED MODEL

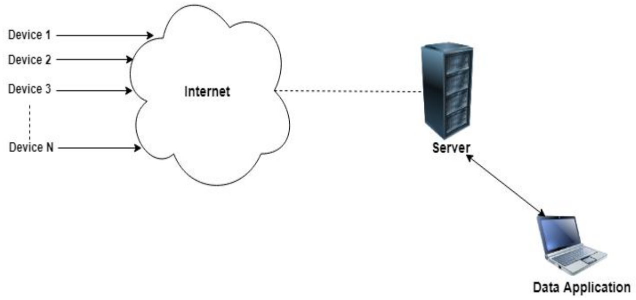


Fig.1: Network model

- The network model consists of several IoT devices, data server, and the internet connection.
- Powerful one-way hash function is available on the public.
- IoT devices are connected openly and not protected physically.
- The data server is considered to be protected.
- IoT devices are has constrained data space and limited processing speed.
- Every IoT device captures multiple data samples and sends them in a single data packet.
- The IoT device data is travelling through the network while there is chances of attacker may alter the data and misuse.
- The altering of data or manipulating the data may cause the wrong decisions, economically loss and human life threat.

The purpose of a digital signature is to verify the authenticity of a data that belong to a sender. This project the public key (Kr) is used to decrypt the data. Both the message and device id is encrypted by the signer using his private key (Kp) to authorizing the authenticated person. Here the digital signature is public key encryption it has a pair of both public and private key. The public key and the private key are related to mathematically each other. But cannot be created from each-other.

The public key is a phenomenon which is available for anyone to decrypt the data. The public key is created to a public key server in public key infrastructure as PKI. A PKI performs sharing, declining and validating public key used for encryption and attaching identities with the public key certificates.

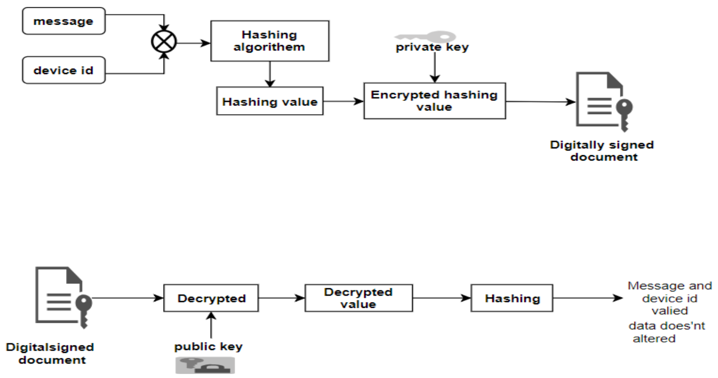


Fig.3: Block diagram of the proposed method

The PKI to authorize the users and systems to protect the data while transferring through the internet and verify the confidentiality of a document. [15]The PKI authenticate the users when transmitting the data is secured by the encryption algorithm. The public key infrastructure certificates append a public key for decrypt and authenticate the data sent from the sender that was provided a certificate in the same way identification information of a sender incorporate in the document with the data and valid period of time. The absence of PKI the delicate data cannot be protected among the parties confidentiality of data.

By the same way, the private key is fixed on the possessor system that cannot be transmitted publicly. The creator of an electronic document is encrypted by the private key i.e. the digitally signing. After that, the receiver decodes the signature with the public key to confirm the attachment is valid.

The private key is unique for both sender and receiver to check the authentication of a sender message. Hashing of a message and then encrypted by the private key is better than the encryption of the whole message for because hashes are the same size of the original message and efficiency is not affected. The entire message is encryption may cause slightly lag the performance.

Here the IoT device sensing data is transmitting through an internet to the third-party cloud services which can store the data. The message (m) and device (id) is hashed by the hashing algorithm to protect the data. The hashing of data is also known as message digest it can be represent as H. The hashing of message and device id is H (m+id).

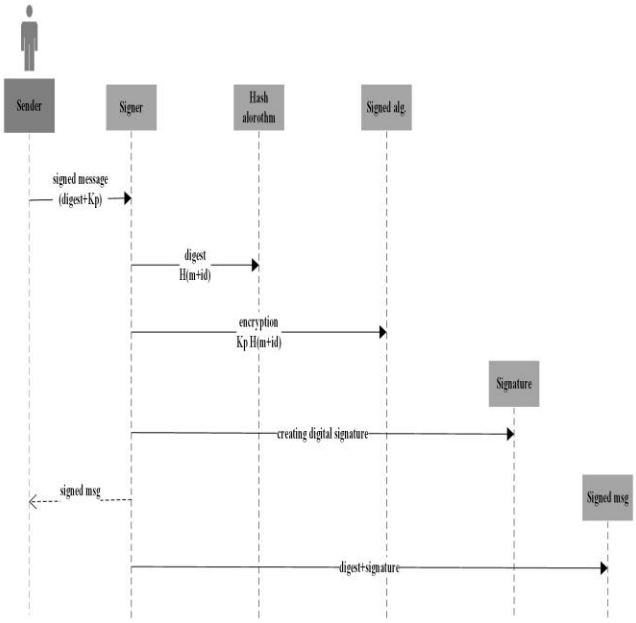


Fig.3: Sender side signing diagram

Here the IoT device sensing data is transmitting through an internet to the third-party cloud services which can store the data. The message (m) and device (id) is hashed by the hashing algorithm to protect the data. The hashing of data is also known as message digest it can be represent as H. The hashing of message and device id is H (m+id).

The hashing value is encrypted by the senders private key Kp and digitally signed by the signature algorithm Kp H (m+id).

The encrypted message is stored in a document and digitally signed by the signing algorithm. The signing of a document with the sender's private key. The digitally signed document is contains the owners information and valid period of time.

The sender sends the message (m) and device identification number (id) along with the sender's private key for encryption purpose.

The both message and device id converted as the digest by the hash algorithm H.

These digest is calculate by the signer and sends it to the signer. The signer encrypts the message digest using the sender's private key with the signature algorithm. Finally digital signature value is obtained.

After these the signer creates the signed document that holds the original data and the signature of the signer. Signer can create the signed document that contains the signature for the document.

Another section the verifier verifies the signature with in the signed document. [16]The signer and verifier use the hash algorithm and signature algorithm to create and check the signature.

The hash algorithm has the hash functions that convert a data to a fixed length of the hash values. The signature algorithm is used for both encryption and decryption by the using the both private and public keys.

By the receiver side the receiver retrieves the public key from the public key repository. After retrieving the key the receiver sends the signed document and sender's public key to verifier.

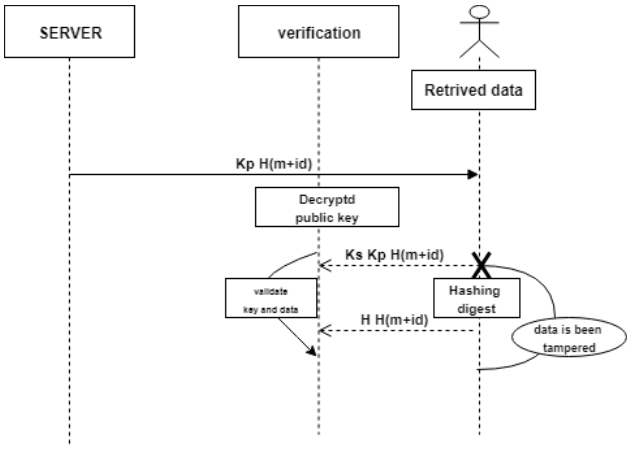


Fig.4: Receiver side diagram

By the receiver side the receiver retrieves the public key from the public key repository. [15][16] After retrieving the key the receiver sends the signed document and sender's public key to verifier.

The verifier decodes the signature using the sender's public key and signature algorithm. The verifier verifies the message digest and simulates the signature and the digest value for the validation purpose.

If the signature and message digest if fails in verifier section the data is altered the verification is not valid.

1. Detecting the altering of data:

This segment recount the propose method for detecting altering of data. The every device has a unique identification number (mac address, serial number, etc.) by using this identification number encounter the data is sensed by which device across through a network. Only using the device id is not perfectly secured so the device id and sensed data or message is summing by a logical operation.

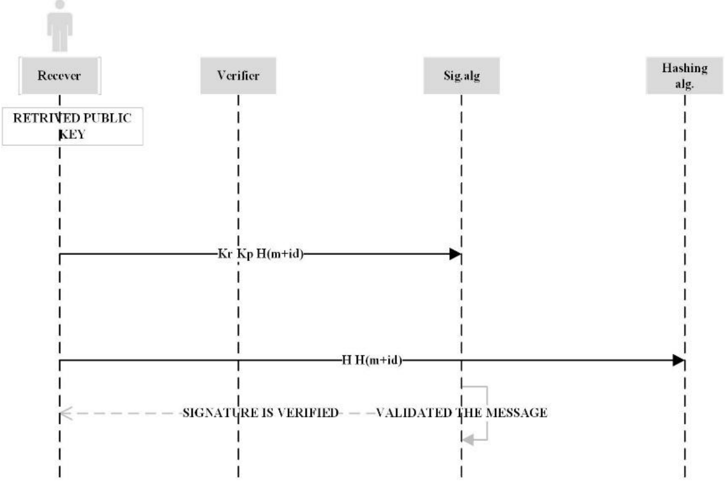


Fig.2: validating the signature and data

The combined data is secured by using hash functions and encryption methods. These encrypted data is transfer through an internet to cloud server.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The cloud server is authenticated by the authorized persons who can access the data. Even this authenticated cloud server has no guarantees of protecting the data. That is the reason behind the verification of both data and signature is must be in the receiver section who wants to get the data.

IV. Results

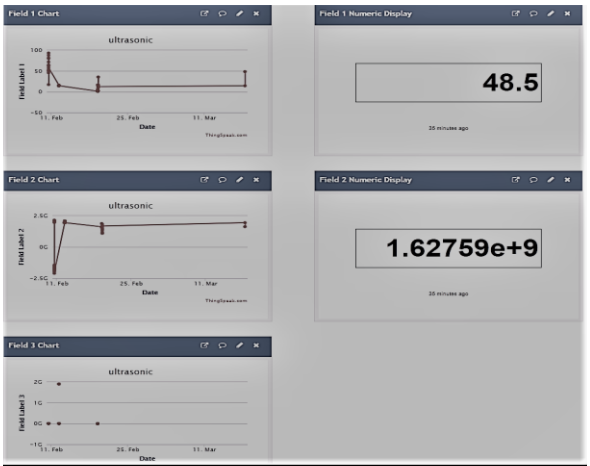
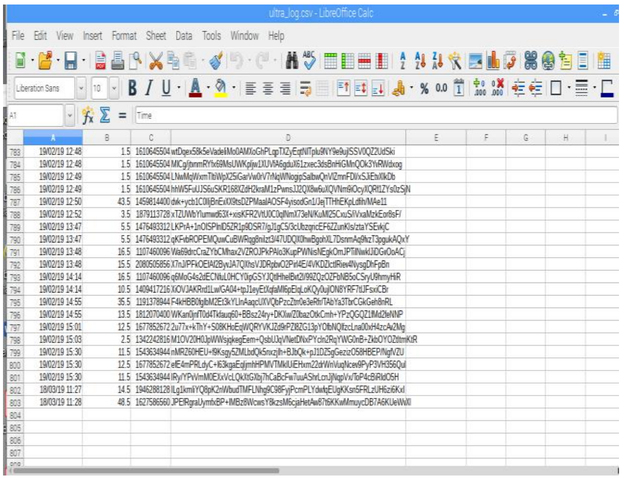


Fig.6: The IoT sensed device data is stored in the cloud

In the cloud server the device id and sensed data is stored in cloud along these hashed data of both device id and sensor data also stored in cloud. The encrypted data is retrieved from the cloud and stored in the local disk. The file is encrypts by the senders private key. These data is stored in the form of hash values.

In the cloud server the device id and sensed data is stored along these data hashed data of both device id and sensor data.



	A	B	C	D
783	19/02/19 12:48	1.5	1610645504	wtDqex58k5eVadeliMo0AMXoGhPLqpTXZyEqtNlTplu9NY9e9ujlSSV0QZ2UdSki
784	19/02/19 12:48	1.5	1610645504	MICg/jtvnmRYfx69MsUWKpljw1XUVfA6gduX61zxec3dsBnHiGMnQOk3YvRWdxog
785	19/02/19 12:49	1.5	1610645504	LNwMqWxmTltiWpX25iGarVw0rV7rNqWNogipSalbwQnVlZmnFDWxSJiEtvXlkDb
786	19/02/19 12:49	1.5	1610645504	hhW5FuUJS6uSKR168XZdH2kraM1zPwnsJJ2QX8w6uXQVNm9iOcyXQRf1ZYs0zSjN
787	19/02/19 12:50	43.5	1459814400	dvk+ycb1C0lljBnEvXX9tsDZPMaalAOSF4yisodGn1/JejTTHhEKpLdfih/MAe11
788	19/02/19 12:52	3.5	1879113728	xTZUWbYlumwd63X+xisKFR2VtU0C0qlNmX73eN/KuMl25CxuS/fVxaMzkEor8sF/
789	19/02/19 13:47	5.5	1476493312	LKPrA+1nOlSPlnlD5ZR1p9DSR7/gJ1gC5/3cUbzqricEF6ZZunKls/ztaYSEvkjC
790	19/02/19 13:47	5.5	1476493312	qKFvbROPEMQuwCuBWRgg8nilzt3/47UDQX0hwBgohXL7DsnmAq9hzT3pgukAQxY
791	19/02/19 13:48	16.5	1107460096	Wa69drcCraZYbCMhax2VZROJPkPAlo3KupPWNisNEgkOmJPTilNwkIJiDGvOoACj
792	19/02/19 13:48	15.5	2080505856	X7nJ/PFkOEtAf2ByvJA7QXhsVJDRpbvO2Pirl4E/4VKDZlctlRiev4NysgDhFpBn
793	19/02/19 14:14	16.5	1107460096	q6MoG4s2dECNfuL0HCY0ipGSYJQtlHhelBvt2l/99ZQzOZFbNB5oCSryU9hmyHiR
794	19/02/19 14:14	10.5	1409417216	XiOVJAKRrd1LwGA04+tpJ1eyEtXqfaMl6pElqLoKQy0ujlON8YRF7tIJFsxiCBr
795	19/02/19 14:55	35.5	1191378944	F4kHBB0fglbM2Et3kYLlnAaqcUXVQbPzcZtn0e3eRft/TAbYa3TbrCGkGeh8nRL
796	19/02/19 14:55	13.5	1812070400	WKan0jnfT0d4Tkfauq60+BBsz24ry+DKXw/Z0bazOtkCmh+YPzQGQZ1fMd2feNNP
797	19/02/19 15:01	12.5	1677852672	2u77x+kThY+S08KHoEqWQRYVKJZd9rPZl8ZG13pYOfbNQlfzcLna00xH4zcAv2Mg
798	19/02/19 15:03	2.5	1342242816	M1OV20H0JpWWsjqkegEem+QsbUJqVNetDNxPYcln2RqYWG0nB+ZkbOYOZtltmKtR
799	19/02/19 15:30	11.5	1543634944	nMRZ60HEU+f9Ksgy5ZMLbdQk5nxzjlh+BJbQk+pJ1DZ5gGeziz058HBEP/NgfVZU
800	19/02/19 15:30	12.5	1677852672	efE4mPRLdyC+l63kgaEqljmhHPMVTMklUiEHxm22drWnVuqNcev9PyP3VH356Qul
801	19/02/19 15:30	11.5	1543634944	IRy/YPvVmM0EXxVcLQkXtGXbj7hCaBcFw7uuAShrLcnJjNqpVx/ToP4cBiRldO5H
802	18/03/19 11:27	14.5	1946288128	ILg1kmliYQ8pK2nWbudTMFLNhg9C98FyjPcmPLYdwfqEUgKKsn5FRLzUH6zi6Kxl
803	18/03/19 11:28	48.5	1627586560	JPEfRgraUymfxBP+lMBz8WcwsY8kzsM6cjaHetAw87t6KKwMmuycDB7A6KUeWvXl
804				
805				
806				
807				

FIG.7: ENCRYPTED AND HASHED DATA IS STORED IN CLOUD RETRIEVED IN A FILE

This is the data retrieved from the cloud and encrypted by the sender by using his private key. The encrypted data is decode by the public key and verified by the verifying algorithm and after both hash value and decode data is valid successfully there is no data is tampered.

V. CONCLUSION

This paper presented a mechanism to identify the data which is received by the authorised system by using the unique identification of the device. The propose method is to secure the device data from the attacks such as manipulation of data and tampering of data. The system is capturing the data from the IoT devices and then stored in a cloud resource for the sake of device has the limited resource. The cloud data is not fully secure even it is authenticate to overcome this problem signature and verification scheme is to secure the data and validate the data is tampered or modified

REFERENCES

1. Andrey Bogdanov, Miroslav Knezevic, Gregor Leander, Deniz Toz, Kerem Varc, and Ingrid, “SPONGENT: The Design Space of Lightweight Cryptographic Hashing”. IEEE 2013
2. Xunjun Chen, Zheng Gong and Yiyuan Luo, “Cryptanalysis of the Lightweight Block Cipher Hummingbird”. IEEE 2013
3. Jun-Ya Lee and Wei-Cheng Lin, “A Lightweight Authentication Protocol for Internet of Things”. IEEE 2014
4. Oriol Pinol, Shahid Raza, Joakim Eriksson, Thiemo Voigt and Stockholm. “BSD-based Elliptic Curve Cryptography for the Open Internet of Things”. IEEE 2015
5. D.Jamuna Rani and S. Emalda Roslin, “Light Weight Cryptographic Algorithms for Medical Internet of Things (IoT) - A Review”. IEEE 2016
6. Manish Kumar, Sunil Kumar, M.K. Das and Sanjeev Singh, “Lightweight Data Security Model for IoT Applications: A Dynamic Key Approach”. IEEE 2016
7. Sanaah Al Salami, Joonsang Baek, Khaled Salah and Ernesto Damiani., “Lightweight Encryption for Smart Home”. IEEE 2016
8. Sriram Sankaran, “Lightweight Security Framework for IoTs using Identity based Cryptography”. IEEE 2016
9. Effy Raja Naru, Dr. Hemraj Saini and Mukesh Sharma, “A Recent Review on Lightweight Cryptography in IoT”. IEEE 2017
10. Vijay Dahiphale, Gaurav Bansod and Jagdish Patil, “ANU–II: A Fast and Efficient Lightweight Encryption Design for Security in IoT”. IEEE 2017
11. Kinza Sarwar, Sira Yongchareon and Jian Yu, “Lightweight. ECC with Fragile Zero Watermarking for Internet of Things Security”. IEEE 2018
12. Maria Almulhim and Noor Zaman, “Proposing Secure and Lightweight Authentication Scheme for IoT Based E-Health Applications”. IEEE 2018
13. Xin Li, Huazhe Wang, Ye Yu and Chen Qian, “An IoT data communication for authenticity and integrity”, IoTDI 2017.

[14].@availale https://searchsecurity.techtarget.com

[15]. @available https://www.gatevidyalay.com

[16]. @available https://www.cryptomathic.com

AUTHORS PROFILE

K.SAMBASIVA RAO M.Tech (Embedded systems) department of ECM in Koneru Lakshmaiah educational foundation at Vijayawada, India.

M.KAMESWARA RAO associate professor Department of ECM in Koneru Lakshmaiah educational foundation at Vijayawada, India.