Efficient Secure Authentication Protocol for 5G Enabled Internet of Things Network

K Praveen Kumar [*], T N S Padma[**], B Pruthvi Raj Goud [***]

[*] Assistant Professor Dept. Of IT, Anurag Group of Institutions Hyderabad, Telangana.
[**] Assistant Professor Dept. Of CSE, Sreenidhi Institute of Science And Technology Hyderabad, Telangana.
[***] Assistant Professor Dept. Of IT, Anurag Group of Institutions Hyderabad, Telangana.

***Abstract*- (IoT)** *The Internet of Things, The scope of Internet of Things is not limited to connecting things including (smart) - homes, cities, environment, energy systems, retails, logistics, industry, agriculture and health. IoT system has a single node/device that performs sensing, performs controlling, performs analysis, host the applications and stores data,. IoT allows those nodes / devices to communicate and exchange information i.e control of machine and flow of information. IoT devices are enabled with 5G network technology. 5G is being developed to provide very large capacity, robust integrity, high bandwidth, and low latency. With the development and innovating new techniques for 5G- IoT, The IoT service access would require a intermediate access network to connect to 5G, and access network may be publicly accessible. Hence, there exists security threat to user's data and services. It wills surely facing the new security and privacy issues. Here we provided an authentication service for node to node communication and data transfer. The protocol is resistant to various attacks, which could originate from Confidentiality, Integrity and Availability. The user-credentials and services-request are secretly communicated, thereby preserving the privacy.*

Index Terms- *Authentication & security,5G Enabled IoT, Cryptography and Cryptanalysis, secret keys.*

I. INTRODUCTION

The IoT is enabled by several technologies like wireless sensor networks, mobile phones, vehicles, , smart city, smart health care, intelligent transport, Industrial Automation, cloud computing, big data analytics, embedded systems, security protocols and architecture, communication protocols, web services, mobile internet, semantic search engines and using in disaster responses. This leads to the production of huge data volumes. Here we have to know technologies play a key role in IoT:

I. **Wireless Sensor Networks**: WSN comprises of distributed device with sensor which are used to monitor the environmental and physical conditions. Wireless networks increased by over a factor of 100 from under 3 Exabytes in 2010 to over 200 Exabytes by 2019. And exceed 500 Exabytes by 2020. The Connected devices will reach 100 billion by 2030. WSNs used in IoT systems are as follows: weather monitoring systems in which nodes are collecting temperature, humidity and other data, which is aggregate and analyzed. Indoor air quality monitoring systems in which wsns to collect data on the indoor air quality and concentration on various gases in the room. Surveillance systems use wsns for collecting surveillance data. Same as Health systems, smart grids and agri systems to collect data from the specified sensor and perform the tasks.

II. **Cloud Computing: C**loud computing is a transformative computing paradigm that involves delivering applications and services over the internet. Cloud computing involves provisioning of computing, networking and storages resources on demand and providing these resources as metered services to the users. Cloud computing resources can be provisioned on demand by the users, without requiring interactions with the cloud service provider. The process of provisioning resources is automated. Cloud computing resources can be accessed over the network using access mechanisms that provides platform independent access through the use of heterogeneous client platforms such as workstations, laptops, tabs and smart mobiles.

The Cloud Computing services are offered to users in different forms. Iaas (Infrastructure as a Service) , Paas (Platform as a Service) , Saas (Software as a Service) .

III. **Big Data Analytics:** Big data is defined as a collection of data sets whose volume, velocity, or variety, is so large that it is difficult to store , manage, process and analyze. Big data Area using IoT , sensor data generated by IoT system such as wether monitoring systems, data collected from sensor embedded in industrial and energy systems, Health and fitness data generated by wearable fitness bands, and data generated by IoT systems for location and tracking of vehicles .

II. RELATED WORK

IV. **5G (Fifth Gen Network Technology)-Enabled IOT:** 5G is being developed to provide extremely large capacity, robust integrity, high bandwidth, and low latency. With the development and innovating new techniques for 5G-IoT, it surely will drive to new enormous security and privacy challenges. Consequently, secure techniques for data transmissions will be needed as the basis for 5G-IoT technology .The requirement of new IoT services , the 5G is coming, which aims to provide a 1000 times higher mobile data per unit area, Ten-Thousand times more connecting devices and data rate, and 5 times reduced latency. In future 5G will become the backbone of Internet of things (IoT).

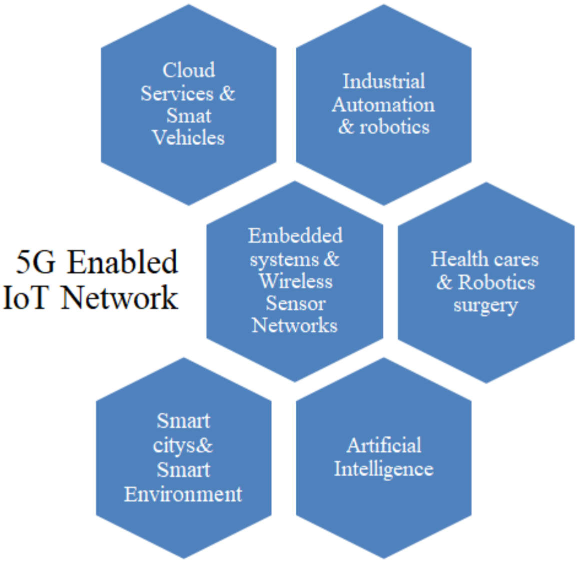

5G Enabled IoT Network
Cloud Services & Smat Vehicles
Industrial Automation & robotics
Embedded systems & Wireless Sensor Networks
Health cares & Robotics surgery
Smart citys& Smart Environment
Artificial Intelligence

Figure 1: 5G Enabled IoT Services

IoT is a technology that includes devices which share data on the internet. Industries ,cities, and homes are changing to the smart with IoT. It incresed the number of devices connected day by day, and it could be huge billions of devices by 2020-2030.

5G enabled IoT consumes less power and less latency. All the IoT services do not require 5G network. 5G network can provide IoT applications with low latency and high reliability of services.

Figure 1 shows some of the 5G based IoT applications and services such as Industrial Automation like connected cars, health care monitoring like wearable devices, smart education, agriculture, smart home automation, smart cities like smat street lights and smat environments, Artificial Intelligence, Cloud services and Wireless networks , there is no cabling required , Ultra –Speed ,Ultra-low latency, Ultra-reliability and Ultra-efficiency is expected in the coming years in between 2020-2030.

Table 1: Comparison between 5G and 4G networks

Sno	Features	5G 2020-25	4G 2010-20
1	Technology	LTE-M, New Radio(NR)	LTE,LTE-A
2	Network Latency	Ultra-Low(below 1ms)	Low(30-70ms)
3	Network speed	Ultra-High Speed	High Speed
4	Network capacity	Ultra-High	High
5	Data rate	10Gbps	50-100Mbps
6	Mobility	Ultra-High	High
7	Spectrum efficiency	Ultra-High	High

III. THE PROPOSED FRAME WORK FOR SECURE AUTHENTICATION PROTOCOL FOR 5G ENABLED IOT NETWORKS.

The Security of the 5G- IoT devices is very complex problem, because the devices having the high bandwidth and high spectrum usage. So the Connected devices will reach 100 billion approximately by 2030.So the devices are communicating and data transferring each other's . IoT system has a single node/device that performs sensing, performs controlling, performs analysis, host the applications and stores data. IoT allows those nodes / devices to communicate and exchange information i.e control of machine and flow of information. IoT devices are enabled with 5G network technology. 5G is being developed to provide very large capacity, robust integrity, high bandwidth, and low latency. With the development and innovating new techniques for 5G-IoT, The IoT service access would require a intermediate access network to connect to 5G, and access network may be publicly accessible. Hence, there exists security threat to user's data and services. It wills surely facing the new security and privacy issues. Here we provided an authentication service for node to node communication and data transfer. The protocol is resistant to various attacks, which could originate from Confidentiality, Integrity and Availability. The user-credentials and services-request are secretly communicated, thereby preserving the privacy.

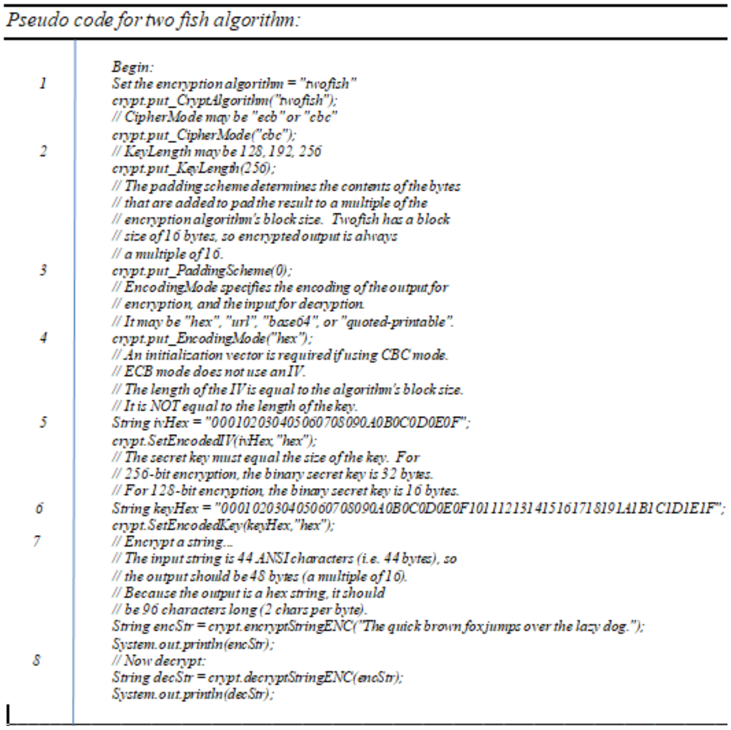
The protection against the intruders or third parties we can propose the secure authentication protocol for verifying the messge or data comes from the particular sender or not, Here we can also provide the cryptography and cryptanalysis.

Internet of Things brings a new set of security issues. IOT devices must be their own strong security, authentication and encryption standards. The IoT devices manufacturing or providing industries know that encryption must be the silver bullet to protect their products and consumers data.

Here we propose the algorithm for encryption and decryption process i.e ***Twofish Encryption Algorithm***

Twofish encryption algorithm is a block cipher algorithm. It is replacement and overcome for the AES. It was designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall and Niels Ferguson.The key length is 128-256 bits and it is very strong and widely used algorithm. This encryption standard is efficient on systems or devices with low capacity processors and IoT device smart cards etc.

Figure 2: Pseudo code for twofish encryption algorithm for confidentiality



Pseudo code for two fish algorithm:

```
    Begin:
1   Set the encryption algorithm = "twofish"
    crypt.put_CryptAlgorithm("twofish");
    // CipherMode may be "ecb" or "cbc"
    crypt.put_CipherMode("cbc");
2   // KeyLength may be 128, 192, 256
    crypt.put_KeyLength(256);
    // The padding scheme determines the contents of the bytes
    // that are added to pad the result to a multiple of the
    // encryption algorithm's block size.  Twofish has a block
    // size of 16 bytes, so encrypted output is always
    // a multiple of 16.
3   crypt.put_PaddingScheme(0);
    // EncodingMode specifies the encoding of the output for
    // encryption, and the input for decryption.
    // It may be "hex", "url", "base64", or "quoted-printable".
4   crypt.put_EncodingMode("hex");
    // An initialization vector is required if using CBC mode.
    // ECB mode does not use an IV.
    // The length of the IV is equal to the algorithm's block size.
    // It is NOT equal to the length of the key.
5   String ivHex = "000102030405060708090A0B0C0D0E0F";
    crypt.SetEncodedIV(ivHex,"hex");
    // The secret key must equal the size of the key.  For
    // 256-bit encryption, the binary secret key is 32 bytes.
    // For 128-bit encryption, the binary secret key is 16 bytes.
6   String keyHex = "000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F";
    crypt.SetEncodedKey(keyHex,"hex");
7   // Encrypt a string...
    // The input string is 44 ANSI characters (i.e. 44 bytes), so
    // the output should be 48 bytes (a multiple of 16).
    // Because the output is a hex string, it should
    // be 96 characters long (2 chars per byte).
    String encStr = crypt.encryptStringENC("The quick brown fox jumps over the lazy dog.");
    System.out.println(encStr);
8   // Now decrypt:
    String decStr = crypt.decryptStringENC(encStr);
    System.out.println(decStr);
```

IV. Taxonomy for the Secure Authentication & Confidentiality of the IoT Transmission:

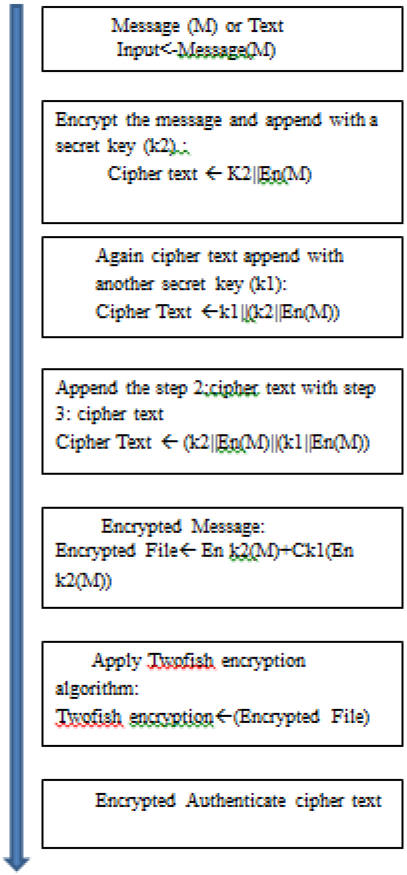

Message (M) or Text
Input<-Message(M)
Encrypt the message and append with a secret key (k2)..:
Cipher text ← K2||En(M)
Again cipher text append with another secret key (k1):
Cipher Text ←k1||(k2||En(M))
Append the step 2:cipher text with step 3: cipher text
Cipher Text ← (k2||En(M)||(k1||En(M))
Encrypted Message:
Encrypted File← En k2(M)+Ck1(En k2(M))
Apply Twofish encryption algorithm:
Twofish encryption←(Encrypted File)
Encrypted Authenticate cipher text

Figure 3: Proposed Efficient Secure Authentication and Confidentiality taxonomy for 5G Enabled IoT

In this proposed algorithm we are provide Efficient Secure Authentication with confidentiality and integrity for the 5G Enabled IoT devices communication. All the devices communicate each other over the public network or common network, 5G network provides high speed , efficient spectrum and high data rates. So the intruders or third party peoples easy to attack and modify the text. IoT devices having less security , hackers or intruders easy to attack device and observe the message or patterns of the message and intentionally or unintentionally modify the text. Our system provides high and efficient secure communication for the devices. Here we use very strong and best encryption algorithm for confidentiality i.e twofish encryption algorithm. And for authentication using efficient secure message function using secret keys like k1,k2. Implement this proposed algorithm in current 4G network ,in coming years it will be implement in High speed networks . Encryption is not enough to secure data adding some additional security i.e authentication, Sender and receivers know what messages are transmit mutually it is important.

But normal sender and receiver communication we don’t know the message comes from the particular sender or not, the intruders hack the sender system and transmit the messages to receiver, The receiver feels the message comes from the authorized sender. In this situation we have option to authenticate message using secret keys. The Intruders or unauthorized peoples, get the information from the network, But they cannot modify or observe the encrypted message from the sender and receiver communication media. The Secret key knows only sender and receivers only.

V. CONCLUSION

The Internet of Things is growing day by day. It has spread from the all the Human and machine related areas like Home, agriculture, Healthcare, Cloud computing and Industrial Automation for monitoring production in efficiency. The devices that connect to the internet, it will be publicly accessible. So must be encrypted and provide secure authentication because of the user personal data and business intelligence data they transmit over the network. The encryption is not enough to secure data transmission, we can add authentication to the devices. The best protection or communication is encryption with authentication over the network. Our proposed algorithms applied in two different mobile apps and observe the result. As a future work, the proposed algorithm can be applied on 5G devices and compared with more works and its deep analysis can be done.

References

[1] Jianbing Ni, Xiaodong Lin, Xuemin Sherman Shen ”Efficient and Secure Service Oriented Authentication Supporting Network Slicing for 5G Enabled IoT”, IEEE Journal in Communications, Vol.36,No.3,March 2018.

[2] Michael haus,Muhammad waqas, Aaron Yi ding,”Security & Privcay in device to device (D2D) communication”,IEEE communication

[3] Deivanai Gurusamy, Deva Priya M, Barmura Yibgeta, Assabu Bekalu “ DDOS Risk in 5G Enabled IoT and Solutions” IJEAT Journal,Vol.8, Issue.5, June 2019.

[4] Muchzizmuslim , Budi Prasetiyo, lamsyah “ Implementation Two fish algorithm for data security in a communication network using library chilkat encryption activex “Vol.84, No.3,Feb 2016,issn 1992-8645,JATIT

[5] Ahmet efe, Esra akso,Neslihan Hanecioglue,seyma nur yalman “ Smart security of IOT Against DDOS attacks” issn 2587-1943, IJIEA2,2018

Authors

First Author – K Praveen Kumar, B.Tech(CSE), M.Tech(CSE), Assistant Professor in Anurag Group of Institutions, Hyderabad . Email id: praveen0507@yahoo.com

Second Author – T N S Padma, B.Tech(CSE), M.Tech(CSE), Assistant Professor in Sreenidhi Institute of Science and Technology, Hyderabad.
Email id : padma.tandu@gmail.com

Third Author – B Pruthvi raj Goud , B.Tech(CSE), M.Tech(CSE), Assistant Professor in Anurag Group of Institutions, Hyderabad . Email id: pruthvirajit@cvsr.ac.in