International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

# Implementation of Secure Cloud Based IoT Communication Using Lightweight Cryptography

**Archana D. Wankhade [1], Kishor P. Wagh [2]**

**Submitted:** 23/08/2023 **Revised:** 11/10/2023 **Accepted:** 24/10/2023

**Abstract:** Internet of things consists of things having unique identification of each device and things are connected to the Internet. Traditional devices which are not associate with internet are now having capabilities to get connected with Internet called smart devices. The backbone to IoT network is internet. IoT devices which are connected to Internet called as resource constrained devices because of having low computing power, limited battery power, limited memory etc. Hence when this constrained devices having sensor transmits data over networks are prone to different types of attacks. To avoid attack on IoT network and maintain confidentiality of data over network, it requires cryptographic solution but due to resource constrained nature of devices in IoT comparing with traditional encryption method Lightweight cryptography is more effective. Hence to make cloud based IoT secure transmission we present Fernet Lightweight symmetric encryption based on AES-128 bit in a CBC mode algorithm and HMAC authentication using SHA256 Hash Algorithm. Comparing with other Lightweight Cryptographic algorithms Fernet is found to be best for securing cloud based IoT communication as it is having Keysize of 256 bits and it can perform both encryption and authentication. In this research paper, we implemented Fernet Lightweight cryptographic algorithm for Encryption, Authentication and Key generation to secure transmission of sensor data generated by IoT devices.

***Keywords****: AES (Advanced Encryption Standard), Fernet, IoT(Internet of Things), Lightweight Cryptography, MQTT protocol*

## 1. Introduction

IoT devices are referred to as “Things” in IoT. These devices have unique Identification and have different capabilities like sensing from remote location, actuating capabilities. These devices collect and process data.For the processing it can be send on cloud based application. Hence after processing it, perform some task locally or at IoT Infrastructure. IoT devices consists of I/O interface for Sensors, Internet connectivity interface, Audio/Video Interface, storage interface. This devices can sense data from sensors which can sense external environment like light, motion, humidity or temperature etc. The sensor data is then communicated to cloud for storage purpose. After processing of data, information is generated and command is given to devices with the help of actuators to perform some actions like ON/OFF the device. Relay switch is connected to IoT Device can perform action of ON/OFF the device based on command received to device over Internet. IoT is not limited to connecting devises to Internet. But while designing application for a user it is required to process on raw data, convert it into meaningful information and extract it into knowledge. So while considering this for example we have data of sensor measurement ((62, 44) ;( 72, 55)) which is generated after weather monitoring. Suppose we have to give meaning to this data we have to add context. Suppose we consider tuple in data which is temperature and humidity measurement for per minute. With this context we can get information of the tuple. Further processing this information in terms of Average Temperature and Humidity for last ten minutes by averaging last ten data tuples. Further to extract knowledge understand the relationship in information. Suppose we set Alert if average temperature in last ten minutes is greater than 110F. So that will be useful for any user to getting and alert on certain conditions and application can be developed on it. Hence IoT has wide range of application like Smart home can have smart lighting, smoke /Gas Detectors, smart cities can have smart parking, smart roads etc.

### 1.1. IoT Functional Blocks

**IoT Devices**: IoT devices consists of sensors, actuators, functions for monitoring and controlling.

*1 Research Scholar, Computer Science and Engineering Department, Government College of Engineering, Amravati, India*
*ORCID ID : 0009-0001-1001-8496*
*2 Assistant Professor, Computer Science and Engineering Department, Government College of Engineering, Amravati, India*
*ORCID ID : 0000-0002-8189-3378*
*archanadwankhade@gmail.com*
*ORCID ID : 0000-3343-7165-777X*
** Corresponding Author Email: author@email.com*

**Communication**: Various protocols like CoAP, MQTT, AMQP used for communication by IoT systems.

**Services**: Services like device monitoring, control, data publishing services are required in IoT architecture.

**Management**: This functional block is to govern IoT system. **Application**: It's an interface for users to monitor and control various aspects of IoT system.

Also IoT network has some capability like i) Collection of data ii) Transmission of data iii) Processing of data and iv) Utilization of data. In first stage that is data collection, in this stage resource constrained devices with the help of sensors can sense or collect information from environment or outside world. In second stage that is data transmission stage which uses Ethernet, WiFi, ZigBee to connect objects and users. In third stage that is data processing, application process the data and obtain useful information .In fourth stage utilization of this information is done. Based on this information certain decisions are made and many initiate commands for taking actions on physical environment.

### 1.2. Cloud for IoT

Cloud computing is a paradigm which can deliver applications and also services over internet. Cloud services can provide computing, networking and storage as per user demand and can provide these services "pay as per requirement" basis. Cloud computing is a IoT enabled technology. Big data of IoT devices can be stored on Cloud. Hence Cloud computing and IoT are two correlated technologies.

### 1.3. IoT Infrastructure and Cloud Storage

In IoT network sensor devices generates big amount of data due to which cloud storage is required to store that data. Analysis of data can be done on Cloud and depending on that actuators get command for doing the task. Cloud based IoT Infrastructure is needed for most of the IoT applications.

## 2. Related Work

A number of researchers from all around the world have worked for cryptographic solution in IoT network regarding security issues in constrained devices. Some related research papers are discussed here for implementation of IoT data transmission using lightweight cryptography.

In [1], the author presented lightweight cryptographic protocols. Also presents analysis and comparative study of popular contemporary cipher. Evaluate block and stream algorithm for security.

In [2], author presents and analysed different Lightweight cryptographic approaches. Lightweight cryptography is the only solution for security and performance in wireless sensor networks. Symmetric and Asymmetric Lightweight cryptographic approaches are presented.

In [3], the author analyses different LWC algorithms. In this paper author found and check different cryptographic algorithms for resource constrained devices.

In [4], the author presented to address comparison of LWC with other current cryptographic algorithms using different IoT platforms and analyse which is useful for limited hardware applications.

## 3. Methodology

### 3.1. Cloud based IoT architecture

As IoT devices increases day by day and these devices generates huge amount of data volumes called Big data. Hence Cloud has been proposed to solution for IoT that can manage this Big data generated by smart devices.

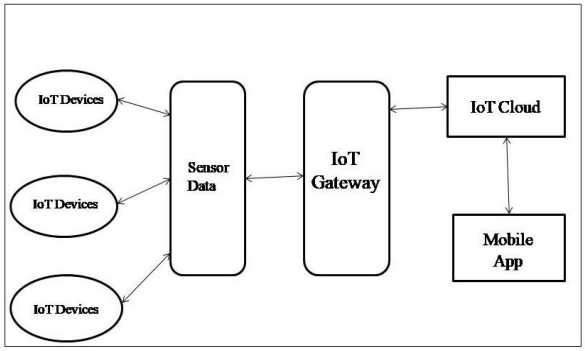


**Fig. 1.** Cloud IoT Architecture

Fig 1 shows following components in Cloud based IoT architecture.

**IoT devices**: Theses are smart devices which can sense real world data with the help of sensor and this sensor data then transmitted through network.

**IoT gateway**: IoT gateway is responsible for transferring this sensors data to cloud for analysis and processing.

**IoT Cloud**: Big data generated by IoT devices can be stored in IoT cloud. Data processing and analysis can be done on this big data for taking decision based on processed information.

**Mobile App**: This can be handled by users to control devices in IoT architecture.

But while travelling this sensors data on wireless network to be stored on cloud it is vulnerable to different attacks.

### 3.2. Types of Attacks

**3.2.1 Passive Threats**: Passive Threats can use data but never affect resources. It affects confidentiality of data. Fig 2 shows how confidentiality of data is affected by Passive Threats.

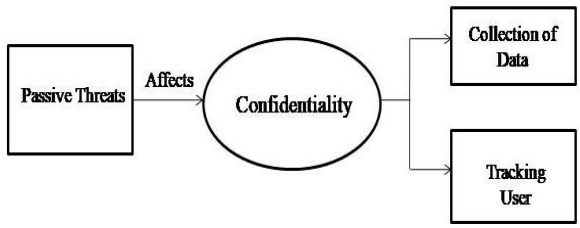


**Fig. 2.** Passive Threats

**3.2.2 Active Threats**: Active Threats attempts to alter data and can take control of hardware or resources. Fig 3 shows security services are affected by active threats.

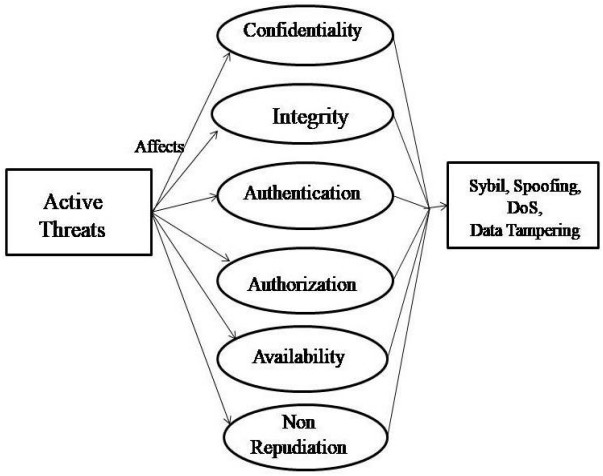


**Fig. 3.** Active Threats

### 3.3. Attacks on different IoT components

IoT attacks can be divided into four categories

#### 3.3.1 Attacks at IoT Devices

Physical Devices consists of sensors, actuators and RFIDs. Sensors can sense data from environment .RFIDs are used in wireless communication with the help of unique identifier. These devices are resource constrained due to which attacks can be easily possible on physical devices .Generally DoS, DDoS can be possible.

#### 3.3.2 Attack at IoT Network

Network service is wireless sensor network with RFID in IoT network. Hence both parts are vulnerable. Possible attacks on RFID include Sybil, synchronization attack and also replay attacks.

#### 3.3.3 Attack at IoT Cloud Service

Cloud computing in IoT architecture facilities to store and obtain information from anytime anywhere. As the system is distributed it is more vulnerable to various attacks like Malicious attack can be done for unauthorized access e.g. SQL injection and cross site scripting. Security attacks or threats can be possible due to inadequate integrity controls. IoT ensure security at Cloud IoT system, these types of security concerns should be minimized.

#### 3.3.4 Attack at Web Application Layer

About all IoT network provides remote access to users using mobile application. The malware designer can hack this system by extracting device information .They can do potential vulnerabilities and also can create botnets. So attacks on different components of IoT architecture which may lead to loose confidentiality, integrity of sensor data. To avoid these types of vulnerabilities on cloud IoT network some robust solutions are required. Theses requires attack detection and mitigation to defend various attacks on Cloud IoT network. Also for secure transmission of sensor data lightweight cryptography can be used.

### 3.4. Traditional Cryptographic Algorithms

**Table 1**: Traditional Cryptographic Algorithms

| | |
|---|---|
| Authentication Algorithm | 1.(MD5)<br>2.SHA-1<br>3.SHA-256 |
| Encryption Algorithm | 1.DES(Symmetric)<br>2.AES(Symmetric0<br>3..RSA(Asymmetric Algorithm) |

For the purpose of protection of data, cryptographic techniques can be used. Some traditional techniques which are used for Authentication and Encryption are listed in Table I.

### 3.5. Lightweight Cryptography for Resource constrained IoT devices

#### 3.5.1 IoT Overview

IoT devices are of two types:1. Rich in Resource like PC, tablets, smart phones etc. 2. Poor in Resources like resource constrained having sensor, RFID tags, actuators etc.Due to the use of this resource constrained devices in many applications these become more and more popular.

#### 3.5.2 Security challenges and Security requirements

As these resource constrained IoT devices interact directly with outside world for purpose of data collection are easily exposed to attack .Attackers can mode these devices as a target .So to make these IoT Network secure different

security requirements can be fulfilled by IoT Network. These security requirements is shows in following Fig 4.

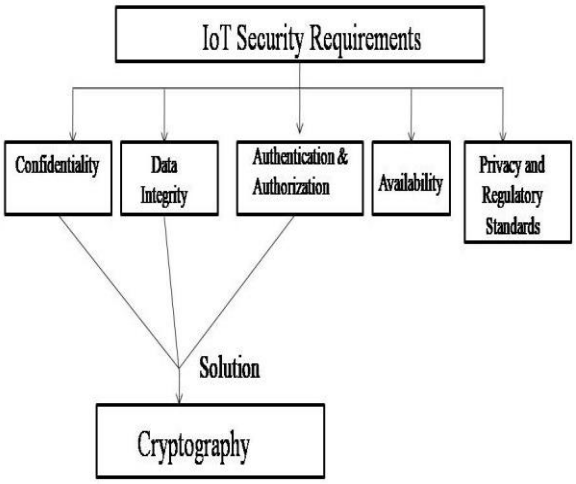


**Fig. 4.** IoT Security Requirements and Solution

In above diagram different IoT Security requirements are explained. Amongst this cryptography can be effective measures to guarantee of data confidentiality, integrity and authentication& authorization of data at the time of transmission .So cryptography can be a solution for secure transmission of data over network as well as secure storage of data. However conventional cryptography algorithms do not suit for IoT Devices which are resource constrained as these requires high resource demand. So it requires lighter version of these conventional algorithm.

### 3.5.3 Challenges in implementing traditional cryptography

Following are some challenges in IoT devices:
1. Limited memory 2.Limited battery power 3.Low computing power 4.Real time response. Limitation in IoT devices make their performance low and not acceptable for traditional cryptography applied on IoT. But all these issues are addressed by lightweight cryptography. One more reason lightweight cryptography is not just applicable to resource constrained devices but it is also applicable to all the devices which are rich in resource which are also involved in IoT network directly or indirectly.

### 3.5.4 Characteristics offered by Lightweight cryptography

Characteristics of lightweight cryptography are as follows.

1. Physical Cost

2. Performance

3. Security

Amongst these first two characteristics are satisfied by LWC algorithms. But the characteristics security is only fulfilled by different internal structure adoption for defending against attacks. These structures are SPN, FN, GFN, ARX, NLFSR, and Hybrid. Following Fig 5 shows structure wise classification of cryptography.

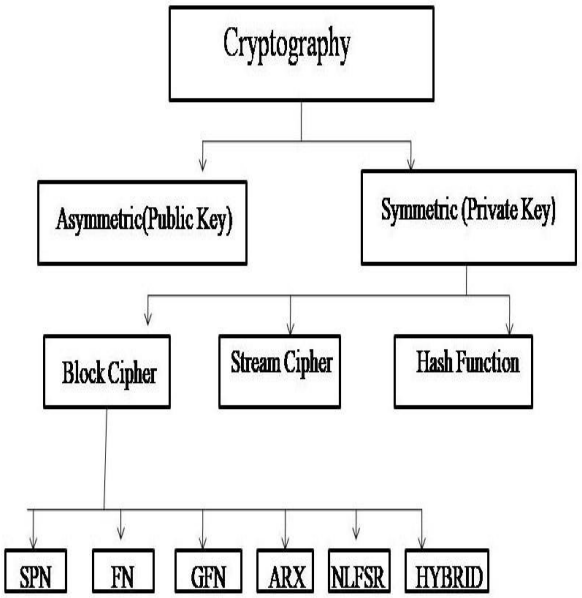


**Fig. 5.** Classification of cryptography

### 3.5.5 Classification of Cryptographic algorithms is in two main categories.

1. Symmetric Key

2. Asymmetric Key

Symmetric key cryptography uses same single key for encryption and decryption but sharing of this key safety is the major issue and which can be solved by using trusted third party. Asymmetric cryptography uses two private public key pairs. It also provides confidentiality, data integrity and authentication of data. In block cipher both encryption and decryption take place on a fixed size block (64 bits or more).But in stream cipher continues processing of input elements is done bit by bit. Two properties are there in cryptography i) Confusion ii) diffusion. It is used to strength the cipher. The confusion is used to make key and cipher text relationship more and more complex by using S-box substitution. The diffusion uses permutation to dissipate plaintext over bulk of cipher text. But stream cipher uses only confusion property and block cipher uses both confusion and diffusion. Hence reverse of encryption for extracting plain text is very difficult in block cipher and easy in stream cipher. Hence block cipher is preferred in resource constrained IoT Devices.

**Table 2**. Comparison of different Types of Cryptographic Algorithms.

| ***Algorithm*** | ***Operation*** | ***Type*** | ***Key size*** |
|---|---|---|---|
| AES | Encryption | Symmetric | 128 bits, 192 bits, 256bits |
| DES | Encryption | Symmetric | 56 bits |
| RSA | Encryption | Asymmetric | 1024 bits, 2048 bits, 3072 bits, 7680 bits, 15360 bits |
| Present | Encryption (Lightweight) | Symmetric | 80 bits, 128 bits |
| Clefia | Encryption (Lightweight) | Symmetric | 128 bits |
| Fernet | Encryption (Lightweight) & Authentication | Symmetric | 256 bits |

Table 2, shows comparison of different cryptographic algorithms. Amongst these in SPN i.e. Substitution Permutation Network AES is a best example having 128 bit block with different keys like 128,192,256 bits. Based on AES 128 bit, Fernet is found to be a best Lightweight cryptographic algorithm because comparing with others Key Size is 256 bits and also it provides both Encryption and Authentication which can be used for securing sensors data of IoT network in terms of confidentiality and integrity.

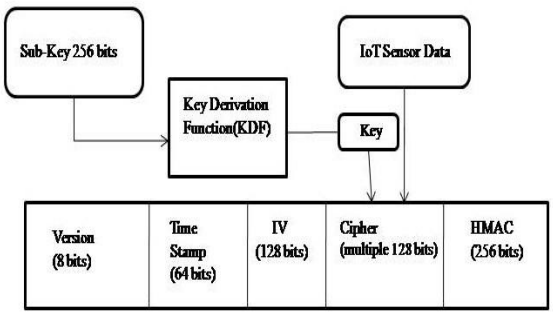


**Fig. 6**. Fernet Symmetric Encryption Architecture

Fig 6. Shows architecture of Fernet Symmetric Encryption. IoT sensors data generated from IoT devices is used as a input for encryption. It requires Key which is derived from KDF. By using Key encryption of IoT sensor data is done and it get encoded to form Cipher text. The same secret key is shared with recipient for authentication and decryption purpose.

## 4. Results and Discussion

In this proposed research work we implemented Fernet lightweight cryptographic algorithm for encryption and authentication of sensor data generated in IoT network using Python. Fernet is a lightweight symmetric cryptographic method which is using symmetric encryption .It is based on symmetric AES-128 in a CBC mode which offers 128 bits multiple length and provide authentication using HMAC with SHA256 Hashing algorithm.

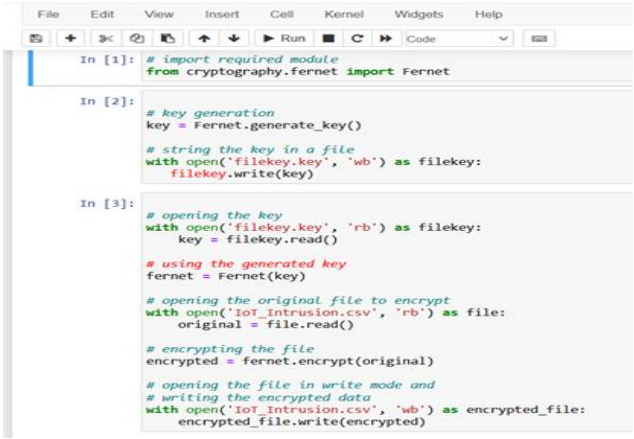


**Fig. 7**. Implementation of Fernet Algorithm

Fig. 7, shows our implementation uses Python to apply Fernet symmetric encryption. Python facilities some libraries for generating keys. Fernet is a lightweight symmetric cryptographic technique which offers encryption as well as authentication. It generates secret key hence it is impossible to decrypt data without key which is shared only with authenticated recipient. Fernet supports private key which is a single key for encryption and decryption .To enhance security in this each character in key undergoes base-64 URL-safe encoding. Encryption procedure performsSubBytes(),RowShifts(),AddRoundKey(),MixColumns() functions. Also reverse of this is for decryption purpose.

## 5. Conclusion

In this proposed research work, we have implemented Fernet lightweight cryptographic algorithm for end to end secure cloud based IoT communication. This ensures a fully encrypted transmission of sensor data which will

resolve a problem of confidentiality and integrity of data to large extent. In this research paper, after doing research on different Lightweight Cryptographic algorithms and Key management systems, we conclude to use Fernet lightweight symmetric cryptographic algorithm because Fernet uses two different algorithms: AES128 bits in CBC mode as encryption algorithm and HMAC using SHA256 authentication algorithm and having Keysize of 256 bits which resolve our problem of secure communication of cloud based IoT network using lightweight cryptography.

## References


[1] M. Rana ,Q.Mamun, R. Islam "Lightweight cryptography in IoT networks: A survey", *Journal Future Generation Computer Systems*,Vol.129,pp.77-89,2022,doi.org/10.1016/j.future.2021.11.011

[2] H. Tawalbeh , S. Hashish ,"Security in Wireless Sensor Networks Using Lightweight Cryptography", in Journal of Information Assurance and Security, ISSN 1554-1010 ,Volume 12, pp. 118-123, 2017.

[3] C. Silva, V. A. Cunha, J. P. Barraca, R. L. Aguiar "Analysis of the Cryptographic Algorithms in IoT Communications",in Springer Information Systems Frontiers, doi: 10.1007/s10796-023-10383-9,2023.

[4] A. Fotovvat, G. M. E. Rahman, S. S. Vedaei and K. A. Wahid, "Comparative Performance Analysis of Lightweight Cryptography Algorithms for IoT Sensor Nodes," in IEEE Internet of Things Journal, vol. 8, no. 10, pp. 8279-8290, 15 May15, 2021, doi: 10.1109/JIOT.2020.3044526.

[5] V. A. Thakor, M. A. Razzaque and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," in *IEEE Access*, vol. 9, pp. 28177-28193, 2021, doi: 10.1109/ACCESS.2021.3052867.

[6] F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686-1721, thirdquarter 2020, doi: 10.1109/COMST.2020.2986444.

[7] Mishra, S.; Albarakati, A.; Sharma, S.K.," Cyber Threat Intelligence for IoT Using Machine Learning", *Journal Processes*,Vol.10,pp.2673 doi. 10.3390/pr10122673.

[8] Sharma, R., Arya, R. Secure transmission technique for data in IoT edge computing infrastructure. *Complex Intell. Syst.* **8**, 3817–3832 (2022). https://doi.org/10.1007/s40747-021-00576-7

[9] Hsing-Chung Chen and Ilsun You and Chien-Erh Weng and Chia-Hsin Cheng and Yung-Fa Huang,"A security gateway application for End-to-End M2M communications", *Computer Standards & Interfaces*,Vol.44,pp.85-93,2016, doi.org/10.1016/j.csi.2015.09.001.

[10] A. Makkar, S. Garg, N. Kumar, M. S. Hossain, A. Ghoneim and M. Alrashoud, "An Efficient Spam Detection Technique for IoT Devices Using Machine Learning," in *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 903-912, Feb. 2021, doi: 10.1109/TII.2020.2968927.

[11] C. Liu, Y. Zhang, J. Xu, J. Zhao and S. Xiang, "Ensuring the Security and Performance of IoT Communication by Improving Encryption and Decryption With the Lightweight Cipher uBlock," in *IEEE* Systems *Journal*, vol. 16, no. 4, pp. 5489-5500, Dec. 2022, doi: 10.1109/JSYST.2022.3140850.

[12] A. Jamalipour and S. Murali, "A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of Things: A Survey," in IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9444-9466, 15 June15, 2022, doi: 10.1109/JIOT.2021.3126811.

[13] A. K. Pathak, S. Saguna, K. Mitra and C. Åhlund, "Anomaly Detection using Machine Learning to Discover Sensor Tampering in IoT Systems," ICC 2021 - IEEE International Conference on Communications, Montreal, QC, Canada, 2021, pp. 1-6, doi: 10.1109/ICC42927.2021.9500825.

[14] G. Said, A. Ghani, A. Ullah, M. Azeem, M. Bilal and K. S. Kwak, "Light-Weight Secure Aggregated Data Sharing in IoT-Enabled Wireless Sensor Networks," in IEEE Access, vol. 10, pp. 33571-33585, 2022, doi: 10.1109/ACCESS.2022.3160231.

[15] R. Sivakumar, J. Jayapriya and N. Krishnan, "Comparison Study on SPN Type Light Weight Cryptography Algorithms for IoT," 2022 International Conference on Inventive Computation Technologies (ICICT), Nepal, 2022, pp. 1051-1055, doi: 10.1109/ICICT54344.2022.9850849.

[16] A. I. Regla and E. D. Festijo, "Performance Analysis of Light-weight Cryptographic Algorithms for Internet of Things (IoT) Applications: A Systematic Review," 2022 IEEE 7th International conference for Convergence in Technology (I2CT), Mumbai, India, 2022, pp. 1-5, doi: 10.1109/I2CT54291.2022.9824108.

[17] Elena Petrova, Predictive Analytics for Customer Churn in Telecommunications , Machine Learning Applications Conference Proceedings, Vol 1 2021.

[18] Dhabliya, D. (2021). Feature Selection Intrusion

Detection System for The Attack Classification with Data Summarization. Machine Learning Applications in Engineering Education and Management, 1(1), 20–25. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/8

[19] Anand, R., Ahamad, S., Veeraiah, V., Janardan, S.K., Dhabliya, D., Sindhwani, N., Gupta, A. Optimizing 6G wireless network security for effective communication (2023) Innovative Smart Materials Used in Wireless Communication Technology, pp. 1-20.