JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 1929-1937
https://publishoa.com
ISSN: 1309-3452

Implementation of Novel Cryptographic Techniques for Mitigating Security Attacks in Iot

Dr. Kuppala Saritha[1], Dr. D. Leela Rani[2], Dr. K. Balaji[3*], Vanlalruata Hnamte[4], Jamal Hussain[5]

[1]Associate Professor, Department of CSE, School of Engineering, Presidency University, Bangalore, India.

[2]Professor, Department of ECE, Sree Vidyanikethan Engineering College, Sree Sainath Nagar, Tirupati, AP, India.

[3]Associate Professor, Department of CSE, B V Raju Institute of Technology, Vishnupur, Narsapur, Telangana, India.

[4]Research Scholar, Department of Mathematics and Computer Science, Mizoram University, Tanhril, Aizawl, Mizoram, India.

[5]Professor, Department of Mathematics and Computer Science, Mizoram University, Tanhril, Aizawl, Mizoram, India

E-mail: [1]saritha.mphil@gmail.com, [2]dlrani79@gmail.com, [3*]balajikcse@gmail.com, [4]vanlalruata.hnamte@gmail.com, [5]jamal.mzu@gmail.com

(**Corresponding Author: [3*]balajikcse@gmail.com**)

Received 2022 April 02**; Revised** 2022 May 20**; Accepted** 2022 June 18**.**

ABSTRACT

With the Internet of Things (IoT), gadgets of all shapes and sizes may exchange data by connecting to the internet. Any item that a child might play with, your car's stereo, or a household appliance could be considered an example. Even at the end of the twentieth century, it wasn't a distinct concept, but over the last two decades, it has become an integral part of our life. Consumers' ability to change and adapt at breakneck speed is a major contributing factor. Sharing a large volume of data amongst various IoT devices has the unpleasant side effect of making these devices a target for hackers and other unethical users who seek to exploit these devices' vulnerabilities. Furthermore, if this data is stolen or misused by hackers, it might have a devastating effect on the entire firm that owns it. Models, schemes, and implementation features of IoT alternate technologies and devices are all brought together in this tutorial. Confidentiality, authentication, data integrity, and service availability are all addressed in terms of hardware implementation efficiency. Modern attacks and hazards, as well as defenses against them, are taken into account. We'll talk about how cryptography research can help address the new security threats posed by IoT devices. The design of IOT must take safety into account from the outset. The Internet of Things (IOT) has three notable characteristics: general perception, dependable transmission, and intelligent processing. A hybrid encryption technique has been devised in this work in order to mitigate security risks while increasing encryption speed and reducing computing complexity. Information integrity, confidentiality, and non-repudiation in data sharing are the goals of this hybrid algorithm for IOT. We have tested our proposed method against RSA and AES and found that our hybrid technique outperforms the rest of the existing methods.

Keywords: IoT , Security, Cryptography, Encryption , Decryption.

1. INTRODUCTION:

'Internet of Things' is a brand-new field of study in the sciences and engineering as well as in public policy. Since its inception in the 1980s, it has become a popular topic for both the news and social media. Internet of Things (IoT) is significant because of the potential for transforming various aspects of our daily lives and the products and services we use. Generally speaking, when we use the term Internet of Things (IoT), we're referring to situations in which a computer's network connections and capabilities include a variety of non-traditional computing devices, such as sensors. The primary goal is to bring together parts of different technologies, including such computers, networks, monitors, controllers, and so on, in order to create new ways of doing things. These common communication models are used in IoT implementations: devices to devices; devices to gateway; devices to cloud; etc. Other well-known sectors include

Ubiquitous Computing and almost all types of connectivity, Computer science Economy, Cloud and Database Systems as well [1].

IoT's primary goal is to revolutionize our way of life by generating as many intelligent gadgets as possible around us to carry out our daily chores and operations. As a result of the Internet of Things (IoT), we now have the concept of "smart houses," "smart cities," and so on. The Internet of Things (IoT) can be implemented on a personal level as well as an enterprise one. As a result of these programs, users have been able to form social interactions. Smart automobiles, smart traffic lights, and smart roads, all enabled by Internet of Things (IoT) technology, are changing transportation. In addition, it has a significant impact on the agriculture industry, breeding, energy management, etc.[2]. Three levels instead of four are used in the IOT system security and the layers of perception, network, and application have been referred to. The authors have also included security concepts and problems, as well as countermeasures for the challenges[4].

For years, a variety of security problems have been examined in depth, including how people perceive security when it comes to data collecting, data transfer, and the provision of protection for software programs. Accordingly, it is impossible to deny the need for powerful protection against any possible attacks or vulnerabilities in the IOT system, and consequently security must be implemented at every feasible layer that makes up the IOT system.. The IoT system is composed of multiple layers, each of which might contain a diverse set of devices, applications, and networks[3].

Cryptographic keys must be managed in systems that use cryptography, according to the IoT architecture's Key agreement criterion. This includes a variety of functions, such as key generation, key exchange, storage, and use, as well as the possibility of key replacement. The level at which the user interacts with the system[24][25]. User-to-user or system-to-system key management is an option. Users need to agree on a key agreement if they are managing their own keys. This is distinct from the necessity of key scheduling, as should be noted. The word "key scheduling" refers to the process of managing the keys within the cipher's operation[4]. When we talk about "Key Management," we're usually talking about things like the key agreement, scheduling, and so on. Key management is essential to the protection of a cryptosystem. Due to the social aspects of cryptography, it is considered to be one of the more difficult aspects. This includes topics like system policy, which can also include various user trainings[23].

The use of cryptography in network and internet security has been around for a long time. Private information and data can be safeguarded using cryptography so that it cannot be accessed by people without the necessary permissions. Communications and data transfers have been made more secure through the use of cryptography. This study examines the security risks associated with Internet of Things (IoT) systems. The specific security vulnerabilities are classified as per the IoT ecosystem domains that are affected or targeted by the security breaches. The proposed and emergent solutions to these problems are then addressed and based mainly on the cryptography research[22]. The discrepancy between the severity of the problems and the state of existing research makes it evident that more effort is needed to create a safe and reliable Internet of Things.

An important countermeasure to the weaknesses that are accessible to hackers is encryption, which assists in achieving secrecy, integrity, and authentication. Sensor devices deployed in areas with so many constraints that such encryption was never applied to general systems are expected to be encrypted by the Iot network of this new era. It is being investigated and developed to address this issue and the needs of devices with limited processing power and resources, which is discussed as one of the demands for the everlasting level of the IoT architecture. Small memory and ROM sizes, power consumption, and processing speed are only a few of the considerations that go into the lightweight cryptography algorithms that have been developed[21].

2. LITERATURE SURVEY:

Security architecture for IoT systems is discussed in this part, which begins with an overview of IoT system tiers and then identifies the specific security requirements for each layer. Layer and need variations are explored in this section of the existing literature as well. The Framework of IOT has been categorized into four tiers by the researchers in their paper.:

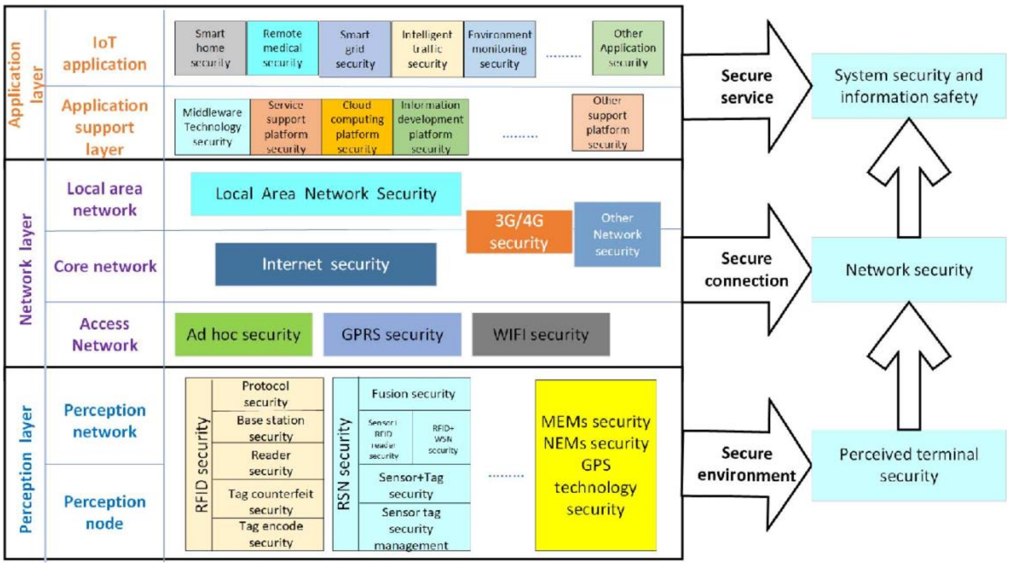

Figure1: Overview of IoT Security Architecture [5]

Perpetual layer, depicted in figure 1, collects various kinds of data first from physical equipment as seen in figure 1. There are a number of basic networks that make up the network layer, which is responsible for transmitting between the devices. These include the internet and wireless networks as well as satellites. Cloud computing and broadband grids will be used to provide intelligent computing power in the support layer. Eventually, the application or user layer delivers services that can be tailored to the user's needs. Their security requirements have been broken down into the various tiers of the architecture. Figure 2 [6] shows the security standards for each layer[20].

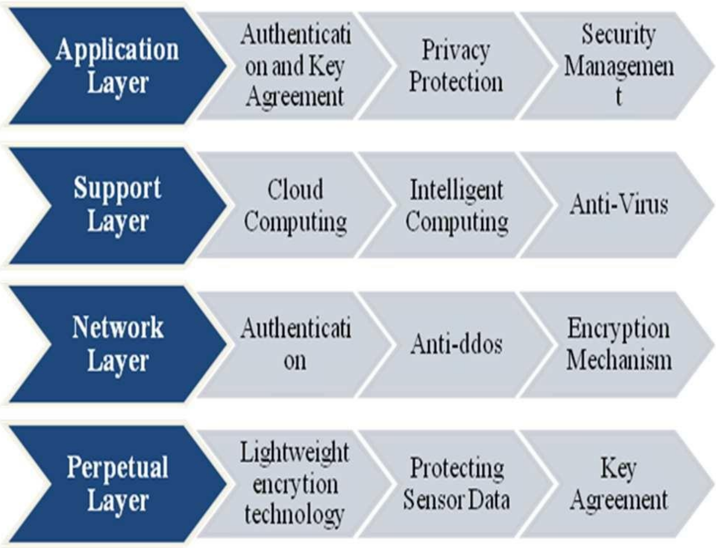

Figure2: Security Requirements at each layer of IOT Security Architecture [6]

The term "hop-by-hop encryption" refers to encoding at the network layer, which means that data in the cipher can be viewed at the nodes where the encryption/decryption takes place. As a result, the nodes should have exceptionally high credit ratings. End-to-end encryption is a word used to describe the encryption that occurs at the application layer, and the data is encrypted at the nodes when this encryption is used. End-to-end encryption is recommended for applications that demand a high level of confidentiality. A standard key management method for a certain compact encryption system will be developed soon in light of the ongoing research into lightweight block ciphers and key management. Figure 1 shows that key agreement and lightweight encryption technology are the foundational requirements of the IoT Security architecture's eternal layer[18][19].

Algorithm-based data encryption is a very well, secure way of transmitting and receiving information and communication. There are numerous ways to decipher [7] because it transforms messages in a variety of ways. These techniques are used to generate cryptographic keys, sign digitally signed documents, and verify the authenticity of digitally signed documents in order to safeguard sensitive data, ensure secure web browsing, and ensure the confidentiality of digital communications including such credit card transactions and email. The development of cryptographic systems, such as AES, Rivest Shamir Adleman (RSA) and Data Encryption Standard (DES), has been facilitated by the better performance of algorithms (DES).

And over 20 billion Internet of Things (IoT) devices will be linked to cloud platforms by 2023, according the latest estimates. Industry IoT (IIoT) applications will account for 63% of the total [6]. As a result, confidentiality and security protection are currently at a standstill. Simple data processing is the primary goal of most Internet-of-things (IoT) devices, such as wearables like the smartwatch and tags that use radio frequency identification (RFID). That's why computers have small screen sizes, poor memory (RAM), slow data rates, limited internal storage, and other drawbacks. As a result of this, Iot systems are still unable to allocate significant memory and processing power just for security operations. Lightweight cryptography (LWC) was created to address this issue [8] since conventional cryptography has become overly complex. This version is designed to run cryptographic algorithms in a small number of CPU cycles while still providing strong resiliency against security assaults.

The LWC is still in the early stages of development. The need for effective LWC solutions is a pressing one in IoT as the data processing requirements of 5GN smart cities grow. Ultra-fast data transfer, low latency and affordability are just some of the benefits that may be gained from implementing a green, low-power, open-source network infrastructure. Thus, our goal is to present a novel LWC optimisation that relies on less on-board storage, less processing resources, and a better battery with the lowest feasible power consumption, all while consuming the least amount of energy. In addition, we want to provide a high level of security and privacy. This paper's initial state provides a compilation of the most recent research in the field. Long-range Internet of Things (IoT) communications are addressed in this work using theoretical and practical techniques in academics and LWC prediction toward Lo-RaWAN [9-10].

LoRaWAN, a cost-effective technology for lengthy IoT networks, is being researched by experts. As a result, it is possible to communicate over distances of up to 20-25 km using low-power media access control (MAC) layer technology. In any security measure in LoRaWAN, encryption is primarily responsible for verifying heftiness in the face of attacks, preventing hazards, and self-recovery with a small chance of failure. LWC, on the other hand, is an innovative strategy, but there isn't enough evidence to support its effectiveness today. There is still a need to examine resource and software defined networking. According to existing research, there are two primary types of LWC: hardware (HW) and computer (SW), which depend on the application's hardware and software skillsets.

Ubiquitous Light Weight Cryptography(LWC) is the foundation of the majority of currently conducted studies. In spite of this, extreme LWC can be implemented using standard resources already in place. As in conventional cryptography, the LWC is divided into two types: symmetric and asymmetric. However, there are only symmetrical development options [11]. For reasons that are difficult to explain, it's not possible to come up with ways to exchange private-public key connections using only a few compute cycles that would leave a minimal footprint. Figure 2 depicts the classification of LWC. At the present, CLEFIA and PRESENT are the most promising block ciphers . While working on LWC block ciphers, some sub-versions of AES and other tweaks have shown to be successful approaches. According to [12, 13,15], some of the LWC algorithms studied in stream ciphers include Grain, Mickey V2 and Trivium. While hash functions are still in their infancy, a theoretical analysis states that a mixture of LWC hash functions with LWC block ciphers will be a suitable suggestion [16] .

3. METHODOLOGY:

A new kind of encryption that can be applied to the Internet of Things is hybrid. Information integrity, confidentiality, and non-repudiation in data sharing for IOT are all supported by hybrid encryption. A hybrid encryption technique called HAN[14] is examined in this study. The proposed algorithm offers unique properties in encryption and decryption, including the ability to produce keys quickly, and it also has the potential to increase internet security by utilizing digital signatures and a number of structures during method construction. The following flowchart depicts the default treatment of tools and equipment in our system design.

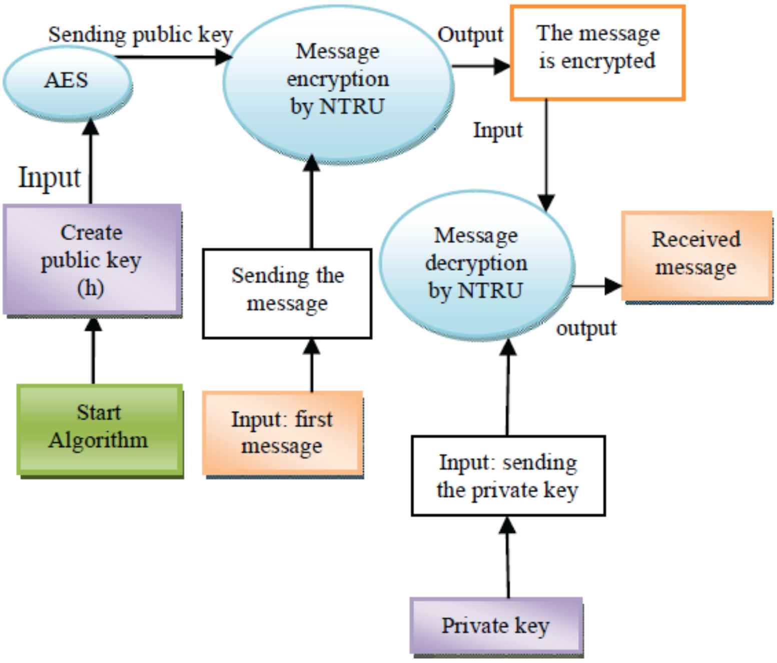

Figure 3: Hybrid Encryption Algorithm Steps(HAN) [17]

A. **Key Creation**:

In AES, a key is created by using the key manufacturing procedure. For the encryption key, a pair of four-by-four matrices known as remain and key are employed. In an XOR operation, we can generate the public key for H by randomly selecting a location from the linear array and a key from the key matrix. In the HAN algorithm, this stage is based on the AEC algorithm. It's important to know that the h key was generated using hexadecimal. Next, we get our hands on the generated public key h. For the purpose of transmitting a secret message from the sender to the receiver, both parties must acknowledge the sender's private key. As a result, the encryption process must be well-secured. It indicates that the sender's encrypted communication will be delivered to the recipient in complete secrecy. Asymmetric NTRU encryption is therefore utilized to improve security. An encrypted message should not be discernible to anyone other than its intended receiver.

B. ENCRYPTION

When a communication is transmitted from one person to another, it is assumed to be received. The message multinomial contains this information. Multinomial messages are sent by selecting a multinomial from the collection, such Lr, and then sending it.

It's important to understand that we can send a message with several Rs. As a result, the sender should keep it a secret.

Encryption □ pr □ h □ message → □□□

Encrypted messages with security capabilities will be sent to the recipient of this message.

C. DECRYPTION

Receiver's private key or encrypting message attempted to open the message when it is encrypted. The NTRU method will be utilized in part for communication decryption in the HAN algorithm. Both f and fp, the receiver's private keys, are in the hands of the recipient. Because fp and f's multinomial are conversing, it is safe to assume that f * fp = 1 will be the message. The receiver multiplies the following message by the value of the parameter a, which comes from the private key:

a □ f □ encryption → □□□

a □ f □ (pr □h □ message) → □□□

a □ f □ Pr □ h □ f □ message → □□□

To choose a correct parameter, coefficients of the poly nominal formula between □q□2 and p□2 are selected. So asp □ 3, then it drastically reduce and does not have any effecton the process, so we can conclude the following relation.

The coefficients of the polynomial formula between □q□2 and p□2 are selected in order to determine the correct parameter. As p decreases to 3, it has no effect on the process, hence we can conclude that the following relation is true.

pr □ h □0 →□□□

a □ f □ message →□□□

The value of b will be determined in the following step. Simply multiply the sender's private key f in the initial message.

a □ b □ f □ message →□□□

Decryption □ (fp □ b) □ x^2 → □□□

Decryption Message is used, we can be certain that the information will be delivered securely to the intended recipient.

D. DIGITAL SIGNATURE

To maintain ID credit in this study, it is preferable to employ digital signatures in conjunction with the given HAN hybrid encryption technique. This is solely for communication integrity and proof of identity and access purposes. In order to perform a digital signature, we must first go from sender to receiver. This means that the sender from step one is now receiver and the receiver is now sender.

Encryption sign □ □message □ f□ □ x^2 → □□□

Decryption □ (h □ 2 □ fp □ Encryption sign) □2 □ h →□□□□

4. RESULTS AND EVALUATION:

In this simulation experiment, the outcomes of the New hybrid encryption Algorithm (HAF) approach are compared with those of the AES and RSA algorithms. Network Simulator NS-2 dynamics simulations are used to assess the HAF approach's efficacy. The parameter under consideration here is Accuracy of Detection.

Detection Accuracy:

Measures the degree of correct detection by the third party (i.e., normal secondary users as normal and harmful secondary users as malicious) of the attack detection accuracy[15]. The accuracy of detection is evaluated in the following manner.

$$D_{acc} = \sum_{i=1}^{n} \frac{SU_i[m/n]}{Nodes} \qquad \rightarrow(11)$$

From the above equation (11), the detection accuracy 'D_{acc}' is measured based on the number of Attack nodes considered for experimentation '$Nodes$' and the administrator correctly detected as malicious or normal.The output is shown in terms of Percentage.

Table 1.Simulation Results of the Attack Detection Accuracy

Number of Data transmission nodes	**Detection accuracy (%)**		
	HAF	**AES**	**RSA**
50	97.6	93.4	89.6
100	95.4	91.2	87.4
150	93.2	89.6	84.2
200	89.6	88.5	81.4
250	87.3	84.6	79.6
300	84.6	81.3	78.4
350	83.7	79.6	76.2
400	82.6	78.4	75.4
450	80.9	77.6	73.5
500	79.6	76.5	71.6

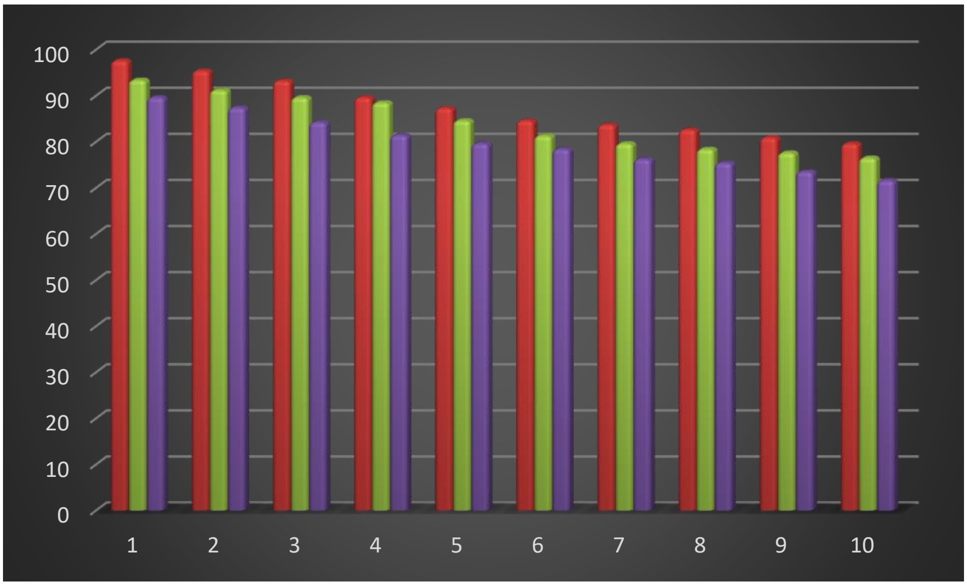

Figure 4: Attack Detection Accuracy Results

The attack detection accuracy obtained for 500 nodes considered for simulation at different period periods is shown in Figure 4. The figure's detection accuracy is not linear in observation. This is showing to the fact that not all nodes are malicious, and only a subset of nodes is considered malevolent. Following the evaluation of trust, a Hybrid Algorithm, is used to distinguish between malicious and non-malicious nodes. As a result, the accuracy of attack detection utilizing the HAF is stated to have increased by 11% when opposed to AES and 16 % when opposed to RSA.

5. CONCLUSION:

Enforcing data confidentiality and integrity has traditionally been used to ensure security in dispersed contexts such as the Internet of Things (IoT). There is a vast attack surface against IoT because of the wide variety of IoT applications, ranging from personal LED light bulbs to entire industrial supply chains. Cryptography has also become important in this field because of the need for security measures such as encryption and non-repudiation in this area. The Internet of Things (IoT) has made great progress, but security and privacy concerns remain open. For IoT services and applications, reliability and security are also critical considerations. We have proposed a hybrid encryption scheme that can improve IOT. IoT security can be improved using the HAN algorithm, which is a hybrid of the AES symmetric encryption and the NTRU asymmetric encryption algorithms. Using this approach, you can generate a key quickly, encrypt or encrypt a message, and decode a message with sufficient security. The correctness of the message is ensured by the multinomial use of this technique in encryption, decryption, and digital signature. Because of the lower level of monetary complexity, this algorithm requires less memory. When compared to the other methods, this one provides encryption in IOT with inferred attacks and an overall increase in security.

References:

[1] D. Miorandi, S. Sicari, F. D. Pellegrini, I. Chlamtac, Internet of things: Vision, applications and research challenges, Ad Hoc Networks 10 (7) (2019) 1497.

[2] H.-K. Lo, M. Curty, and K. Tamaki, “Secure quantum key distribu-tion,” *Nat. Phot.*, vol. 8, pp. 595–604, July 2018.

[3] W. Wootters and W. Zurek, “A single quantum cannot be cloned,”*Nature*, vol. 299, pp. 802–803, September 2020.

[4] P. Hamalainen, T. Alho, M. Hannikainen, and T. D. Hamalainen, “De-sign and implementation of low-area and low-power aes encryption hardware core,” in *9th EUROMICRO Conference on Digital System Design (DSD’06)*, Aug 2018, pp. 577–583.

[5] Zhang, Jian et al. “Overview of IoT Security Architecture.” *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)* (2019): 338-345.

[6] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: a review,” in 2012 international conference on computer science and electronics engineering, 2019, vol. 3, pp. 648–651.

[7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptog- raphy,” Rev. Mod. Phys., vol. 74, pp. 145–195, March 2018.

[8] W. J. Buchanan, S. Li, and R. Asif, “Lightweight cryptography methods,” Journal of Cyber Security Technology, vol. 1, no. 3-4, pp. 187–201, 2017.

[9] J. Darivandpour and M. J. Atallah, “Efficient and secure pattern matching with wildcards using lightweight cryptography,” Computers & Security, vol. 77, pp. 666 – 674, 2018.

[10] C. Manifavas, G. Hatzivasilis, K. Fysarakis, and K. Rantos, “Lightweight cryptography for embedded systems – a comparative analysis,” in Data Privacy Management and Autonomous Spontaneous Security, J. Garcia-Alfaro, G. Lioudakis, N. Cuppens-Boulahia, S. Fo- ley, and W. M. Fitzgerald, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2019, pp. 333–349.

[11] E. R. Naru, H. Saini, and M. Sharma, “A recent review on lightweight cryptography in iot,” in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Feb 2017, pp. 887–890.

[12] K. Tsai, Y. Huang, F. Leu, I. You, Y. Huang, and C. Tsai, “Aes-128 based secure low power communication for lorawan iot environments,” IEEE Access, vol. 6, pp. 45 325–45 334, 2018.

[13] S. Naoui, M. E. Elhdhili, and L. A. Saidane, “Enhancing the security of the iot lorawan architecture,” in 2017 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN), Nov 2016, pp. 1–7.

[14] A. Yousefi and S. M. Jameii, "Improving the security of internet of things using encryption algorithms," *2017 International Conference on IoT and Application (ICIOT)*, 2017, pp. 1-5, doi: 10.1109/ICIOTA.2017.8073627.

[15] Ganesh, D, Thummala Pavan Kumar, and Malchi Sunil Kumar. "Optimised Levenshtein centroid cross-layer defence for multi-hop cognitive radio networks." *IET Communications* 15, no. 2 (2021): 245-256.

[16] Davanam, G., Kumar, T. P., & Kumar, M. S. MULTIPLE NASH REPUTATION CROSS LAYER CLASSIFICATION FRAMEWORK FOR COGNITIVE NETWORKS.

[17] T. Pavan Kumar, and M. Sunil Kumar. "A Dynamic and adaptive learning mechanism to reduce cross layer attacks in cogntive networks." *Materials Today: Proceedings* (2020).

[18] Kumar, M. S., & Prakash, K. J. (2019). Internet of things: IETF protocols, algorithms and applications. *Int. J. Innov.*

Technol. Explor. Eng, *8*(11), 2853-2857.

[19] Sangamithra B, Neelima P, Kumar MS. A memetic algorithm for multi objective vehicle routing problem with time windows. In2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE) 2017 Apr 27 (pp. 1-8). IEEE.

[20] Davanam, Ganesh, T. Pavan Kumar, and M. Sunil Kumar. "Novel Defense Framework for Cross-layer Attacks in Cognitive Radio Networks." *International Conference on Intelligent and Smart Computing in Data Analytics*. Springer, Singapore, 2021.

[21] Balaji, K., Kiran, P. S., & Kumar, M. S. (2020). Resource aware virtual machine placement in IaaS cloud using bio-inspired firefly algorithm. *Journal of Green Engineering*, *10*, 9315-9327.

[22] Ganesh, Mr D., M. Tech, M. Sunil Kumar, and VV Rama Prasad. "IMPROVING NETWORK PERFORMANCE IN WIRELESS SENSOR NETWORKS." *Integrated Intelligent Research (IIR), International Journal of Web Technology* 5, no. 01 (2016): 58-61.

[23] Kumar TP, Kumar MS. Efficient energy management for reducing cross layer attacks in cognitive radio networks. Journal of Green Engineering. 2021;11:1412-26.

[24] Ganesh, D., and M. S Kumar. "Improving Network Performance in Wireless Sensor Networks: A Survey." *Int. J. Web Technol* 5.1 (2016).

[25] V. V. R Prasad. "Mutual Trust Relationship Against Sybil Attack in P2P E-commerce." *Innovations in Computer Science and Engineering*. Springer, Singapore, 2017. 159-166.