Journal of Advances in Science and Technology
Vol. 20, Issue No. 2, September-2023, ISSN 2230-9659

An Analysis of Implementable Security Algorithms in the internet of things Envioronment

Reenu Shukal[1]*, Dr. Gaurav Khandelwal[2]

[1] Research Scholar, University of Technology, Jaipur, Rajasthan

Email: shukal.reenu@gmail.com

[2] Professor and Supervisor, University of Technology, Jaipur, Rajasthan

Abstract - In the scientific community, the Internet of Things (IoT) is the latest buzzword. We live in an age where Internet access is not only possible for the vast majority of the population, but also increasingly affordable. The number of gadgets with internet access and built-in sensors continues to rise. Indeed, the prevalence and prevalence of smart phones, and the use of such devices, are on the rise. With this idea, anybody can hook up any device to the web. However, a major security issue will arise from the practise of storing and communicating data with anyone and any device. It's also unclear how well data can be transferred, communicated, and shared in this setting. In this paper, we discuss concerns about IoT security, including those of privacy, reliability, and accessibility. The rapidly evolving applications made possible by the IoT have drastically altered daily life, making it feel more fantastical and akin to living in a virtual world. Due to its open nature, the Internet of Things (IoT) might pose significant security challenges. A variety of methods, including encryption, are employed to protect the information transmitted by IoT devices.

Keywords - Security, IoT, Envioronment, Algorithms.

- x -

1. INTRODUCTION

The term "Internet of Things" (IoT) refers to a network of interconnected devices such as personal computers, robots, mobile phones, and other gadgets. It's possible for the devices to exchange data with one another because they're all equipped with some form of electronic, software, sensor, and network connectivity and have their own unique identifiers. Any item that can obtain an IP address and use that address to communicate with other items online is potentially part of the IoT. These gadgets can monitor their environments, collect data, and share that data with other devices. A growing number of people feel as though they are living in a simulation because of the proliferation of the Internet of Things. Due to the IoT's goal of connecting everything online, a massive amount of information will be generated, or "big data." Capacity, or the amount of storage required for storing data, is one subcategory of big data; others include data generation velocity, variety of data sources, and data variety. Because IoT allows for global access to data, security is a major hurdle that must be overcome.[1]

As can be seen in Figure 1.1, there are three distinct components that make up the IoT: the sensing layer, the network layer, and the application layer. There is a physical layer called the Sensing layer that is linked to numerous sensors including RFID, WSN, GPS, NFC, and cameras, among others. All sorts of environmental information may be gathered by using these sensors. Additionally, it is effective at transforming raw data into high-quality signals that can be communicated over a network with relative ease. Data from the Recognition layer can be prepared by the Network layer (also known as the Transport layer). In addition, it can use modern data transfer protocols like wired, wireless, and LAN connections to get information to the application layer. The most widely used transmission modalities include 4G and 5G networks, Wi-Fi, Bluetooth, infrared, and so on. The information processed by the lower layers is utilised by the application layer. Information about the program's unique benefits is communicated to the customer in this way. Smart grids, smart cities, and wearable health monitoring are just a few examples of the many uses described for the Internet of Things.[2]

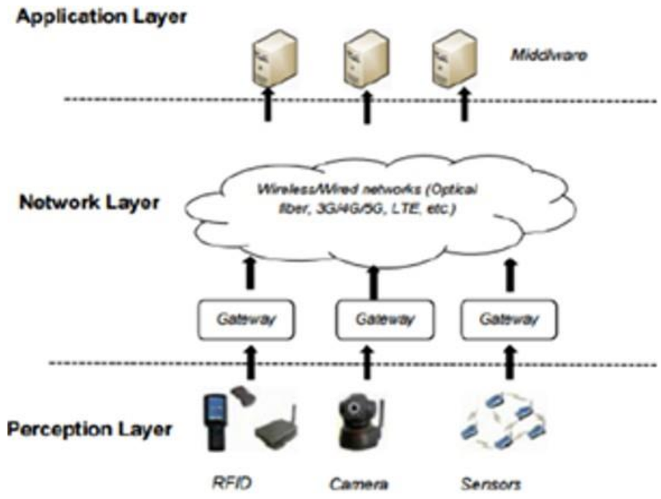

Figure 1.1 – IoT Layers

1.1 IOT Concepts

The Internet of Things (IoT) is seen as a revolutionary technological upheaval that will shape the future of communications and computers in a variety of settings. Nowadays in the digital world, the term "Internet of Things" (IoT) is used as a buzzword. Programmers at Melon University in the early 1980s hooked up a Coke machine to the Internet, making it the first such device. Kevin Auston coined the phrase "Internet of Things" in 1999, the same year the concept of the Internet of Things saw widespread adoption for the first time. The "Internet of Things" is creating a digital representation of physical objects, both alive and inanimate. Connecting sensors to physical items and exchanging data about those objects and their environments through a network is a key component of the Internet of Things. By making it easier for objects to share data via a network, IoT has quickly become an indispensable technology. The success of the Internet of Things is due to the confluence of multiple new technologies rather than any one of them acting alone. The Internet of Things provides huge improvements in convenience all around us. All non-living items that share data via a network are considered active participants in the Internet of Things, alongside the live things that interact. Anything that can send or receive data via a sensor network is part of the Internet of Things. With everything taken into account, the amount of space needed and the strain on the network will only rise. [3]

1.2 Security Analysis of IOT

As the Internet of Things (IoT) grows and develops, it faces new issues in areas like as security, privacy, adequate spectrum, size, and complexity as it links together a growing number of tagged things. Key difficulties that have been identified when examining numerous IoT applications across diverse domains are presented: [4]

i. Privacy

In order to connect its devices, the IoT makes use of numerous wireless networking protocols and a wide range of object identification systems. Consequently, commonplace objects have identification tags that convey object-specific information; this raises concerns about privacy and the need to safeguard against unauthorised access.

ii. Network Security

Since a large number of sensor devices are transmitting data over a wired or wireless transmission network, it is essential that the network be secure to prevent data loss due to congestion and outside interference.

iii. Secure Data Storage

The various sensors involved in the process each collect their own data. The data is sent to the central computer for analysis. Data privacy and security at the I/O node require a robust encryption system, which should be standard on all sensor devices.

iv. Dynamic Cognitive Spectrum

In order for several sensors to share a wireless network and exchange data, each sensor needs its own frequency band. Due to spectrum scarcity, a dynamic cognitive spectrum allocation technique that allows billions of sensors to communicate wirelessly is required.[5]

v. IOT Greening

As more and more devices become Internet-enabled, the demand for network energy will rise sharply in the not-too-distant future. The use of green technologies to improve the efficiency of network devices is thus essential. Smart homes, smart cities, smart businesses, smart agriculture, smart planets, and so on are just some of the places where the Internet of Things is making its mark.

1.3 IoT Applications

The Internet of Things (IoT) is becoming increasingly pervasive due to its numerous uses in several sectors, such as agriculture, commerce, transportation, healthcare, government, and more. Crop fertilisation and harvesting are two applications of GPS tracking and guidance utilised by the agricultural sector. The Internet of Things (IoT) is used in many different and expanding fields.[6]

i. Personal and Home

The Internet of Things (IoT) is making it easier to connect and control appliances in the home, such as refrigerators, lights, air conditioners, washing machines, televisions, and more. Sensing data is protected and can only be accessed by the network's owners. Typically, high-bandwidth and high-sampling-rate data transfers (audio, video, sound) rely on WiFi as the backbone technology. Smartphones, in addition to some interfaces like Bluetooth, can be used to communicate with sensors that measure physiological parameters. The system sends an email to the owner when an intrusion is detected. The task is completed by saving the logs of intrusions in a Google spreadsheet stored in the owner's Google Drive. When an intrusion is detected, the ADXL345 accelerometer detects the door's motion and sends the information to Amazon Web Services IoT.

ii. Smart Health Monitoring

Smart health is making its imprint on the global healthcare industry. Through the use of sensors located in various parts of the body, the Internet of Things is paving the way for a more proactive approach to health care. Applications of the Internet of Things (IoT) in the healthcare sector include patient monitoring and tracking, personnel tracking, identifying medical equipment, and data collection. The RFIDLocator web app employs radio frequency identification technology to supply services to smart health-enabled medical facilities. Medical facilities increasingly use radio frequency identification (RFID) tags for patient tracking, personnel identification, and patient identification and monitoring. An RFID label with a unique identification is attached to the back of every other item. Monitoring heart rate as part of smart health offers great potential for growth in the near future. The integration of sensors and alerts in mobile health helps limit the potential for human mistake and allows for more timely medication administration. WSN4QoL is a Marie Curie project that proposes using new WSN-based technologies in smart healthcare applications, with the aim of improving quality of life for patients. The tracking and communication capabilities of WSN testbeds are enhanced by a network coding and distributed localization solution. [7]

iii. Smart City Concept and Services

Urban IoT, with the aid of sensors installed in buildings, can offer a decentralised database of measures of building structural integrity. Stress in structures, vibrations in the ground, levels of air pollution, local temperatures, and relative humidity may all be detected and recorded by sensors. This opens the door for smart municipal maintenance and improvement programmes. The best possible solutions are provided with less time, money, and effort expended by humans. IoT is introduced for smart city development from three different domains: first, "network-centricnIoT," corresponding to communications; second, "Cloud-centric IoT," analogous to management; and third, "Data-Centric IoT," relating to computation needs.

- Condition of Buildings from a Structural Perspective.
- Taking Care of Garbage.
- We're Keeping an Ear to the Air and the Noise Floor.
- Congestion in the Traffic.
- Consumption of Energy in a City.

iv. Smart Mobile

The concepts of "smart transportation" and "smart logistics" are intertwined with "smart mobile Separating this Internet of Things application is necessary since it will need its own data sharing and backbone infrastructure. Concerns related to traffic congestion, air pollution, and noise pollution fall within this IoT area since they can negatively impact air quality and contribute to greenhouse gas emissions. With the use of a mobile IoT app, we can keep tabs on the shipping vehicles and their cargo, allowing us to streamline our operations and cut down on costs. Freight delays and failed delivery schedules are directly attributable to the negative effects of traffic congestion on the efficiency, productivity, and just-in-time operations of the supply chain. Better and more efficient preparation can be achieved if real-time traffic data is made available.[8]

2. LITERATURE REVIEW

Al-Enezi, K. A., and Alenezi, A. Y. (2018) A lot of people have been working very hard lately to solve the privacy and security issues that plague the Internet of Things. There have been a lot of studies and papers written about the problems and threats associated with IoT security. The survey by Yang et al. illustrates the safety and personal difficulties with remedies that are directly tied to low-end technologies. The security concerns and obstacles facing IoT networks, devices, and systems are briefly discussed by a variety of writers. The surveys by Weber, Gopi, and Rao discuss the difficulties and issues related to security in four stages: (1) the constraints of IoT devices, such as the inability to extend their battery life; (2) lightweight com putation; (3) the categorization of security attacks; and (4) the control of access mechanisms and architecture. Different levels of the Internet of Things's architecture are also discussed (presentation, network, transport, and application).[9]

Mohammadi, M. and Ayyash, M. (2015) The survey by Weber addresses security and privacy concerns, and the study presented by the team includes a security architecture for IoT-based devices. The Internet of Things (IoT) devices are becoming increasingly popular worldwide; these devices incorporate other cutting-edge technologies that are frequently employed all over the world to ship items from one region to another. There is a clear sense of familiarity with this technology. The low-end gadgets have a variety of sensors built in, can communicate with one another, and relay data and information. Security and privacy concerns are the biggest obstacles to using IoT solutions. It's a major challenge to manage all that data so that computers can analyse it safely and reliably. The security, privacy, and privacy of persons are likewise threatened by these IoT. The authors of this study address the increasing need for proper regulation and technicality to bridge the gap between automated monitoring by IoT-based devices and the legally protected rights of individuals who are ignorant of the dangers to their privacy posed by these technologies. Aleisa and Renaud detail the fundamentals of IoT privacy, the dangers to that privacy, and some potential remedies.[10]

Weeks, B., and Wingers, L. (2015) The author offers an Internet of Things middleware as an additional layer between the cloud app and the IoT devices, reducing the cloud's workload. The author employs Attribute-based encryption in the middleware to ensure that users may access all of their data securely from the cloud. Only users who meet the criteria that an administrator specifies as an attribute are granted access to cloud data in an ABE system. If the admin changes the attribute ((X A Y) Z) to need both X and Y, then every user attempting to access the cloud storage must either have X and Y or simply Z. At that point, the information can be understood. One example of ABE is the Cipher text-policy attribute-based cypher. Only authenticated users will have secure cloud access using the CP-ABE method. There won't be any need to do bilinear pairing calculations, which is a significant computational burden. User data will be protected from prying eyes by instituting a Central Attribute Authority (CAA) between the middleware and data owner.[11]

Bhardwaj, I., Kumar, A., and Bansal, M. (2017) In the CP-ABE scheme, a single administrator is in charge of key distribution and also acts as a coordinator to thwart any possible collusion attacks. The entities that will be a part of the access control scheme are the data owner, the middleware, the data users, and the central attributeauthority. The primary benefit of the CP-ABE scheme is that the secret key is only given out to verified users based on the attributes they already possess. The CAA is in charge of the approved user list and attributes, and the CAA only receives approved users from the middleware. Accordingly, it is impossible for hackers and other malicious actors to bypass the middleware and gain access to CAA directly. Attribute's secret key cannot be used for decryption by an invalid user, as CAA prevents access. The model is safe in that sense. The AVISPA tool is presented to further support the proposed scheme.[12]

Devalal, S. and Karthikeyan, A. (2018) In the article, the author suggests using OAuth, an open authorization standard, to gain access to the middleware with just a login, password, and token. The initial step is for the device to sign up with the middleware and create a cloud-based storage folder. In the event that an IoT device submits an authentication request, the gateway will perform a check using the available REST API. At last, the gateway will pass along its own credentials to the exposed API in order to provide access to the request. The request itself contains input parameters like the secret key and the gateway ID. The next step is for the API to verify the request by checking the user's credentials and granting or denying access. After the gateway has been granted permission, an encrypted form containing information about the device is delivered back to it. If the information in the form is valid, the gateway issues the device an access token. The device and gateway will now be able to exchange data in real time. [13]

3. METHODOLOGY

The proposed architecture is a variant of the BRIGHT family of small block cyphers. Since decryption is as easy as encryption, BRIGHT is a Generalized Feistel Network with only four branches and relatively simple round functions. With a low decryption overhead and a proven safety margin, it's an attractive option. In software, shorter key lengths and smaller block sizes leave less of a buffer against brute-force search attacks. Thus, 64-bit minimum key sizes and 80-bit minimum block sizes have been established for the BRIGHT family of block cyphers. The term "lightweight" is used to describe a security method that is not just suitable for a platform with constraints, but also works well on other platforms. The proposed family of BRIGHT cyphers provides good performance on several platforms thanks to its design, which is independent of the underlying application. As a result of the wide diversity of devices and uses, the proposed cypher provides a wide range of options for both block size and key size. Block sizes of 64 bits and 128 bits are the most popular, whereas key sizes vary depending on the level of security needed; for instance, a low-cost device may be safe with only 64 bits of a key, while more sensitive applications may require 256 bits. We designed BRIGHT to work with blocks as little as 64 bits and as large as 128 bits in size. There are a total of three key sizes, and the block sizes range from 80 to 256 bits. We begin by trying to estimate the minimum number of rounds "R" needed to carry out full diffusion for each iteration of the BRIGHT family, so as to provide a sufficient security buffer against existing attacks. The proposed cypher satisfies SAC from the first round onwards; specifically, the BRIGHT family cyphers shift around half of their bits per round. It takes little more than 8 cycles for any cypher in the BRIGHT family to spread. BRIGHT 64/96 has 4R+1 rounds because the number of rounds in each subsequent variant is calculated by adding one to the number of rounds in the previous variant, using the formula 4R. This ensures the safety of the cyphers from any potential attacks. High resistance to related-key attacks on key scheduling is provided by the BRIGHT family of cyphers. This map is characterised by the many operations performed on it, such as circular shift, XOR, and modular addition. Each round ends with a permutation, increasing randomness and disorientation significantly. Initial round key whitening, in which the key is XORed before it is utilised in the round function, is employed because to the ease with which the block cypher with obvious weakness may be mapped when non-linear operations of cyphers rely on the real key values. The effect and manipulations of the one-round function Rki are shown in Figure 3.1.

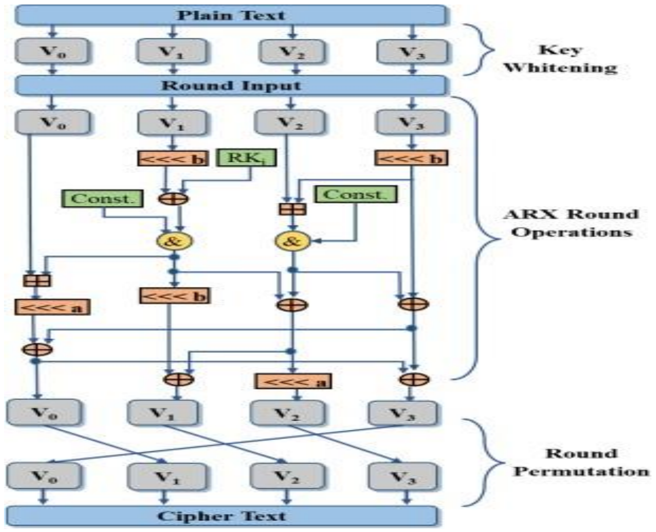

Figure 3.1: Structure of BRIGHT cipher

Decryption makes use of the same round function as encryption, but with the round keys, operations, and constants executed in the opposite order. Several researchers have employed key whitening to protect against a variety of dangers with great effectiveness. With the use of the key whitening concept, we can protect ourselves from weak key attacks like SIT. When it comes to analytical attacks, such as linear and differential cryptanalysis, key whitening is largely ineffective. It makes MITM attacks more difficult to pull off and makes brute-force attacks more challenging to pull off as well. To accomplish key whitening in the first round, the BRIGHT family of cyphers makes use of a sub-key.

The above map is used to describe the processes performed by the cypher. Each stage of encryption and decryption consists of four distinct layers. There are four distinct phases: the round permutation stage, the pre-key-whitening stage, the ARX round operations stage, and the post-key-whitening stage. First, the supplied plain text is split into two words, or branches, of equal length. Once the first layer has these two words, it may begin the prewhitening process on the keyboard. The layer below receives as input the data processed by the layer above it. After the initial key whitening in the first layer, the two words are transferred as a round input to the second layer, where ARX-based operations are performed. Operations on the second and third levels are repeated "R" times, where "R" is the number of iterations. Structure of the UBRIGHT-suggested encryption is seen in Figure 3.2.

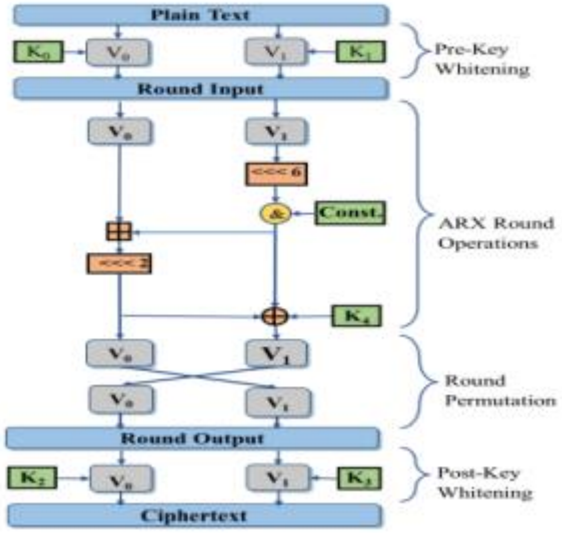

Figure 3.2: Layers in the UBRIGHT cipher

The operations of the proposed UBRIGHT cypher are made to prevent most forms of attack. Using ARX-based cyphers in software is more efficient than any other parallel processing method. The proposed UBRIGHT cypher is efficient in its dissemination because of the way in which the modular addition, XOR, and circular shift operations are arranged. Combining XOR with addition modulo 2 n is a common application. When combined with additional operations, non-linear processes like addition modulo 2 n propagate differences indefinitely at the same pace as bitwise XOR.

4. RESULT

Most devices in the Internet of Things are able to exchange data with one another and with more complex servers in the cloud. Given these constraints, it's necessary to automate certain processes, such data collection from sensors or inventory counts. It follows that 64-bit CPUs should be adequately quick to process lightweight block cyphers. It's important to have block cyphers that are both secure and versatile enough to perform effectively on a number of different platforms. The results of implementing the proposed BRIGHT family of lightweight cyphers on a 2.40 GHz Intel (R) Core (TM) i5-2430M CPU are displayed. IoT-based devices have a number of drawbacks, such limited processing power, memory, battery life, etc. A significant difficulty for IoT applications with limited resources is the often little amount of memory available on most IoT devices. An analysis of how much memory the proposed BRIGHT cypher takes up Memory use for the BRIGHT family of cyphers is compared to that of other lightweight block cyphers based on ARX that are already in use on the same platform in Figure 4.1. (64-bit processor).

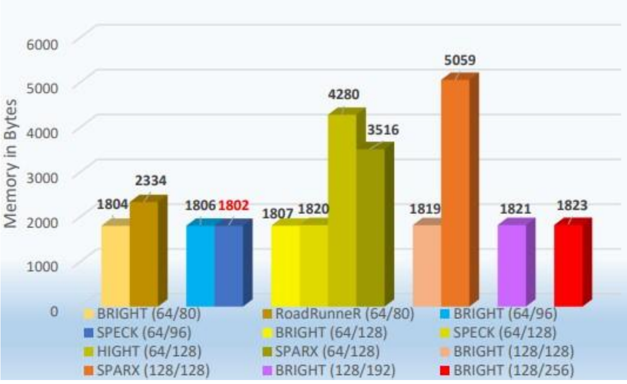

Figure 4.1: Memory analysis of standard ARXblock ciphers with BRIGHT family implemented on a 64-bit platform

The proposed BRIGHT family of cyphers is suitable for application in IoT since it requires less memory than current cyphers. While it is possible to further reduce the amount of the code, doing so would result in a drop in performance. While loop unrolling can improve register utilisation and speed up an operation, it does so at the price of increasing the amount of memory required to carry out the process. Therefore, a loop unrolling intermediate concept may be used to obtain symmetrical performance. Everything is dependent on the needs of a particular use case. The BRIGHT family cyphers use the least amount of flash memory, with the exception of the version with a block size of 64 and a key size of 96. SPECK (64/96) uses less memory than BRIGHT (64/96). Despite having the lowest flash memory of any family, the SPECK family is vulnerable to a number of assaults because of the complexity of its construction. Of these attacks, differential and linear attacks are two examples.

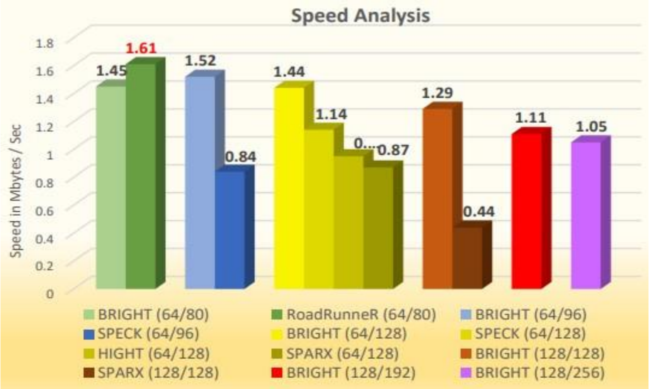

Figure 4.2: Speed analysis of standard ARX-block ciphers with BRIGHT family implemented on a 64-bit platform

They are both written in C on a 64-bit CPU, and their settings are compared in Figure 4.2. This was done so that the results of the BRIGHT cypher and comparisons to other cyphers are not skewed by platform-related artefacts. Every member of the BRIGHT family, with the exception of the RoadRunneR (64/80), has quicker execution times than the other existing lightweight ARX cyphers. Thanks to dynamic key scheduling, the RoadRunneR cypher can decrypt messages rapidly. In addition, RoadRunneR's potential vulnerability in key attacks may stem from its reliance on simplistic key scheduling. The speed of BRIGHT cypher can be improved, but only at the cost of greater memory. To address this, the proposed BRIGHT cypher incorporates a speed-to-memory tradeoff into its design.

incremental progress toward achieving the IoT's potential and protecting it from harm. The efficiency of the proposed family of lightweight cyphers is measured in a number of ways. On 64-bit platforms, the recommended family cyphers perform worse than any other benchmarked cypher save for Road Runne R (64/80), but on 32-bit platforms, the suggested cyphers perform better than any similar LBC. All of the suggested family cypher variations have the least flash memory use, with the exception of the version with a 64-bit block size and 96-bit key size.

5. CONCLUSION:

To guarantee the authentication system is secure, we are developing a middleware that sits between the user and the IoT environment and ensures that users are only connected to the IoT environment after passing numerous authentications, even if the attacker is successful in retrieving the secret key. As important values evolve over time, they become increasingly resistant to threats. On addition, the user and the IoT device must have a safe way to interact with one another without the risk of a data breach, and all of this information must be recorded in a distributed ledger utilising blockchain technology for future verifications. The Internet of Things is an interdisciplinary field where cutting-edge technology meets everyday people to boost both workplace satisfaction and output. With the proliferation of IoT devices comes the need to manage, connect, and work together with a centralised server/gateway, all of which are being met by an explosion of new technologies.

REFERENCES

1. Charnes, C., & Pieprzyk, J. (2018). An algebraic analysis of Trivium ciphers based on the boolean satisfiability problem. In Proceedings of the 4th International Workshop on Boolean Functions: Cryptography and Applications, pp. 173-184.
2. Hao, Y., Bai, D., & Li, L. (2015). A meet-in-the-middle attack on roundreduced mCrypton using the differential enumeration technique. In International Conference on Network and System Security, pp. 166-183.
3. Biham, E., Anderson, R., & Knudsen, L. (1998). Serpent: A new block cipher proposal. In International workshop on fast software encryption, pp. 222-238.
4. Matsui, M., Moriai, S., Nakajima, J., & Tokita, T. (2000). Camellia: A 128-bit block cipher suitable for multiple platforms—

design andanalysis. In International Workshop on Selected Areas in Cryptography, pp. 39-56.

5. Leander, G., Toz, D., Varici, K., & Verbauwhede, I. (2016). Spongent: The design space of lightweight cryptographic hashing. IEEE Transactions on Computers, 62(10), 2041-2053.
6. Dutta, I. K., Ghosh, B., & Bayoumi, M. (2019). Lightweight Cryptography for Internet of Insecure Things: A Survey. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0475-0481.
7. Biryukov, A., Velichkov, V., & Le Corre, Y. (2016). Automatic search for the best trails in ARX: application to block cipher speck. In International Conference on Fast Software Encryption, Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), 9783(2008), 289- 310.
8. Hu, S., Philip, N. Y., & Sungoor, A. (2016). The potential of Internet of m-health Things “m-IoT” for non-invasive glucose level sensing. In 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 5264-5266. IEEE.
9. Al-Enezi, K. A., and Alenezi, A. Y. (2018). Improving the cost factor of dlbca lightweight block cipher algorithm. Indonesian Journal of Electrical Engineering and Computer Science 10, 2, 786–791.
10. Mohammadi, M. and Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials 17, 4, 2347–2376.
11. Weeks, B., and Wingers, L. (2015). The simon and speck lightweight block ciphers. In Proceedings of the 52nd Annual Design Automation Conference. 1–6.
12. Bhardwaj, I., Kumar, A., and Bansal, M. (2017). A review on lightweight cryptography algorithms for data security and authentication in iots. In 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC). IEEE, 504–509.
13. Devalal, S. and Karthikeyan, A. (2018). Lora technology-an overview. In 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA). IEEE, 284–290.

Corresponding Author

Reenu Shukal*

Research Scholar, University of Technology, Jaipur, Rajasthan

Email: shukal.reenu@gmail.com