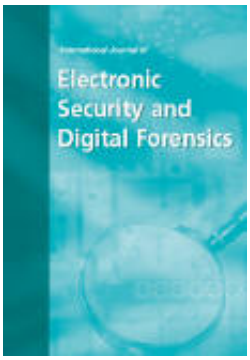


International Journal of Electronic Security and Digital Forensics

ISSN online: 1751-9128 - ISSN print: 1751-911X
https://www.inderscience.com/ijesdf

Security of internet of things based on cryptographic algorithm

Sonam Mittal, Soni Singh, D. Balakumaran, K. Hemalatha

DOI: 10.1504/IJESDF.2024.10052834

Article History:

Received:	15 July 2022
Accepted:	05 October 2022
Published online:	12 January 2024

Security of internet of things based on cryptographic algorithm

Sonam Mittal and Soni Singh

Department of Computer Science and Engineering,
Chitkara Institute of Engineering and Technology,
Chitkara University,
Punjab, India
Email: Sonam.mittal@chitkara.edu.in
Email: sonisingh0107@gmail.com

D. Balakumaran

S.A. Engineering College,
Chennai-77, India
Email: balakumaran@saec.ac.in

K. Hemalatha*

Department of Electronics and Communication Engineering,
Kongu Engineering College,
Erode, India
Email: khemalatha.ece@kongu.edu
*Corresponding author

Abstract: The desire for automated and connected gadgets has managed to become more significant as the globe continues to advance. The internet of things (IoT), a brand-new idea that focuses around the idea of smart gadgets, has been launched in order to address the situation. The results of this analysis are then used to intelligently govern the operational behaviours of these devices. This study fills this need by describing the design, construction, and practical assessment of a fast deployable internet of things architecture that includes embedded data security. We demonstrate that cryptography that depends on the randomness of wireless link is a great option for the IoT technology. We conclude by discussing the challenges and issues that encryption algorithm is now facing and making recommendations for future research in an effort to make key generation a trustworthy and secure defence against the IoT technology.

Keywords: safety; internet network; cross-layer security; cryptography; cryptographic algorithms; computer hacking.

Reference to this paper should be made as follows: Mittal, S., Singh, S., Balakumaran, D. and Hemalatha, K. (2024) 'Security of internet of things based on cryptographic algorithm', *Int. J. Electronic Security and Digital Forensics*, Vol. 16, No. 1, pp.28–39.

Biographical notes: Sonam Mittal is a PhD scholar in the Department of Computer Science and Engineering (CSE), Chitkara University, Punjab, India. She had completed her graduation and Master's degree from the CRSCE and DCRUST, in 2009 and 2011 respectively. She is having more than seven years' experience of teaching. Her research areas include wireless sensor networks, cloud computing, and cryptography. Currently, she is currently working on an enhanced homomorphic encryption algorithm to preserve privacy in the cloud environment.

Soni Singh is a PhD candidate in the Department of Computer Science and Engineering, Chitkara University, Punjab. She has been doing research in artificial intelligence, machine learning, and deep learning since 2017. Her current research is concerned with the prediction of pandemic outbreaks using machine learning and deep learning techniques. She has worked on the Pregaura project for the women's healthcare system.

D. Balakumaran received his BE in Electronics and Communication Engineering in 2004 from the Arunai Engineering College, Tiruvannamalai affiliated to Madras University and ME from the SSN Engineering College affiliated to Anna University, Chennai, India. He has 12 years of teaching experience and two years of industry experience in VLSI design, and currently working as an Assistant Professor in the Department of Electronics and Communication Engineering, S.A. Engineering College, Chennai, India. His research interests include VLSI design and wireless communication. He has contributed in many papers in national and international journals. He is a member of ISTE professional society.

K. Hemalatha is currently working as an Assistant Professor in Electronics and Communication Engineering Department, Kongu Engineering College and has ten years of experience. She is a Fellow member of IETE and her areas of interest include signal and image processing, VLSI signal processing, soft computing and deep learning.

1 Introduction

Individuals, objects, and the surroundings are all integrated through the internet of things (IoT). IoT will revolutionise everyday life thanks to innovative new applications, such as home automation, b2b, networked hospitals, and intelligent structures, to mention just a some of them, as shown in Figure 1 (Al-Fuqaha et al., 2015; Burg et al., 2018). Because of its profound effects on the economy and civilisation, the IoT has garnered enormous technology development attention from both academic and industry. According to a McKinsey prediction, there can be 25–50 billion gadgets in use by 2025, with a potential annual economic effect of $3.9 trillion to $11.1 trillion (Manyika et al., 2015). The internet of everything (IoE) may be used in a variety of industries, including automated farming, transport systems, home automation, and smart transportation infrastructure (Figure 1). The IoE often struggles with its limited storage and processing capacity restrictions, which compromises device efficiency, privacy, and security (Kamil, 2018; Majid and Ariffin, 2019; Gubbi et al., 2013; Hasan et al., 2020). Given the widespread use of IoE in modern culture, it is critical to increasing compliance and security.

The software application might be used for societal good, commerce, health, or individual need. Constrained application protocol (CoAP), developed by Shelby et al. (2014) and is used to meet the minimal resource requirements of the IoT network.

IoT could be viewed as a prevailing inter-network made up of numerous diverse entities, both online and offline, including people, detectors, applications, and various types of devices. These entities are connected to one another at practically any level through special addressing strategies and engage in a variety of interactions. It is anticipated that IoT will open the door for ground-breaking applications in a variety of fields, including medicine, remote monitoring, public transit, and industry. Singh et al. (2014) suggested that it will also be able to integrate techniques like innovative machine-to-machine interaction, autonomous networking, judgement, confidentiality protection, and safety, as well as cloud technology with innovative tracking and actuation techniques.

A larger sample size is guaranteed and necessary processing/computation of information are done at the gateway level to lessen strain on the lower level. The points for info collection and data retrieval come next in the grade. Data is saved and processed for servers that do higher level computation at this level. At this level, the data is evaluated, stored, and presented in such a manner that further working on the data is made simpler, thus increasing the data's significance for higher level programs and end users. The programs that gather the data from a data centre after it has been evaluated and offer the analysis of that input, which is subsequently utilised by end users for certain reasons, are the last ones.

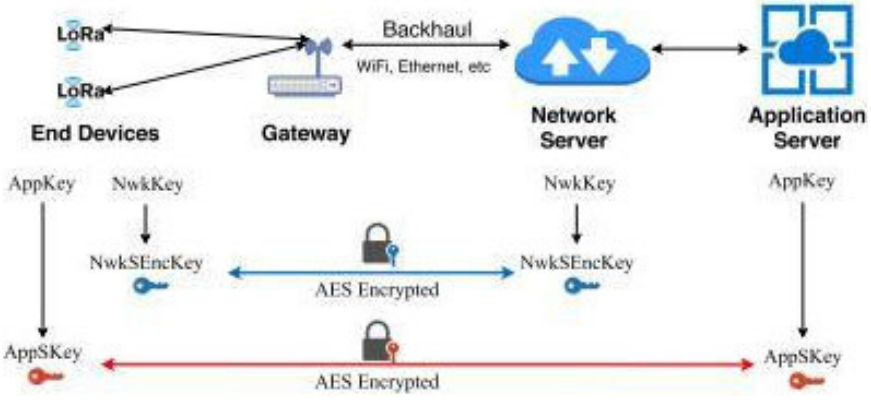
2 Literature survey

Encryption techniques, encryption process, advanced encryption standard (AES), and hash functions may all be generically categorised as three distinct kinds, according to Pérez et al. (2012). Despite being adaptable, asymmetric cryptographic algorithms demand more power, storage, and processing time, making them unsuitable for protecting IoT applications. Stream and block ciphers are two types of symmetric encryption encoding that are suited for IoT applications because they are quick and employ simple procedures. Block ciphers are more adaptable in terms of application, while stream ciphers are faster but better suited for streaming data. For the security of resource-constrained devices in IoT applications, a number of these light-weight block ciphers have been developed. Zhang et al. evaluated several wireless sensor network (WSN) standard security techniques and power use. The central server (BS) processes the data that the WSN nodes provide it, and if any more processing is necessary, relays it to the cloud. The AES algorithm overhead during encryption and decryption was approximated by Xiao et al. (2006) in microseconds. According to Shi et al. (2013, 2015), research efforts have been undertaken to accomplish hardware authentication protocol generation concurrently. Though not widely applicable, the suggested technique is only relevant to wireless BANs and requires that both devices be put on the same individual using LoRaWAN as an illustration. Figure 1 shows how the most recent LoRaWAN standard, version 1.1, has provided a strict security system.

Other IoT protocols, like LoRaWAN, avoid defining how to deliver encryption keys to authorised users. Although PKC are commonly used on the web, it may face difficulties in the internet environment. It is presumable that these devices are diverse in

nature with a range of resource and performance needs. These devices play a crucial role in a secure IoT-based network since it is at this level that data integrity and authenticity are determined. The graphic shows that the next component is a gateway for sending and receiving data out of a cloud platform.

Figure 1 The LoRaWAN procedure provides security measures (see online version for colours)



Notes: Connection and application session encryption is done via AES. However, there is no information on ways to distribute access keys, particularly application key and network key.

Numerous options for securing devices with limited resources are provided by current research. IoT designs for particular applications have been developed by Appel et al. (2016), Eisenbarth et al. (2012), Bogdanov et al. (2007), Beaulieu et al. (2013) and Mahajan and Sachdeva (2013). However, no research has looked at these concerns together and offered information on how encryption impacts an IoT platform's performance as a result of system memory, time, and energy use. This study aims to analyse the impacts and consequences of encryption techniques for IoT applications by combining such topics into a single work.

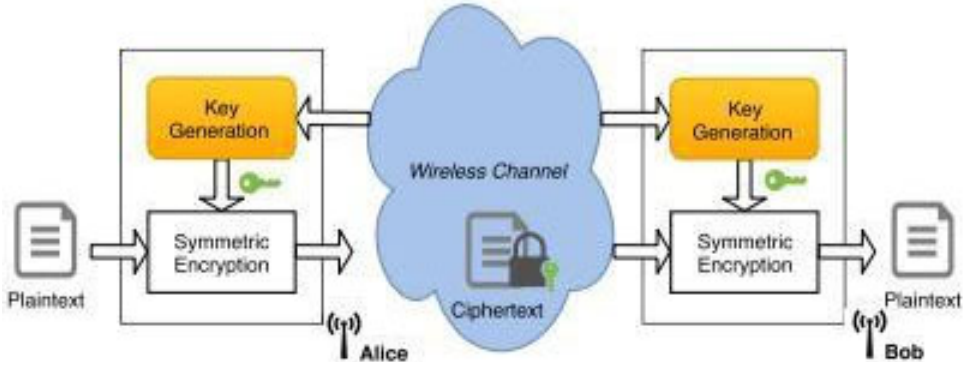
3 Methodology

The integrated CPU in the second layer aggregates the environmental parameter data from the first layer's sensors and actuators, which operate as input devices. The wireless communication module, which connects the sensor nodes wirelessly using technologies like Bluetooth Low Energy (BLE), Wi-Fi, and ZigBee, makes up the third layer. In order to cover a vast region, these wireless technologies often build a form of mesh network. In this study, we first offer a mathematical system model in order to appropriately use these strategies for reference IoT-based system. Next, we provide a method for adaptive selection. This selection technique makes use of theoretical modelling process optimisation formulae that account for weighted resource and throughput restrictions of the target IoT devices.

The algorithm chooses the appropriate implementation method for a certain device or gateway based on these limitations and the values of the various AES approaches and methods that are currently available. In order to increase the overall performance of the

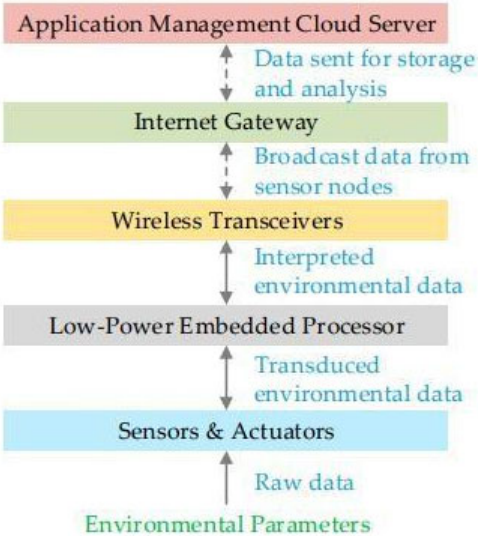
IoT-based system while adaptively reducing the resource utilisation of IoT devices, this approach is applied to several of IoT devices. The next parts of the study provide further information on the numerical system model, adaptive decision mechanism, and matching method. This work offers a thorough analysis of wireless channel-based random key generation. We present the principles of key generation, such as evaluation measures and strategies for system modelling. Figure 2 illustrates a comprehensive key generation procedure that is suggested to take use of the shared randomisation of communication networks between two respectable users.

Figure 2 A hybrid encryption scheme with a key generator process (see online version for colours)



Notes: The identical events key is established for 'Alice' and 'Bob' through data encryption. Once symmetric encryption is complete, they utilise the key.

Figure 3 Communications and architectural design in an IoT (see online version for colours)



In certain situations, the 2nd and 3rd layers are combined into one because the embedded systems layer contains an integrated information stack. A small number of wireless transceivers adhere to strict communication protocols and security standards, while the bulk does not when a consequence, the data is vulnerable as it transitions from the data transmission component level to the connection layer. This may be analogous to how electronics compilers employ their optimisation function. Despite how great and beneficial, program algorithms are certain increased refinement will always need human input.

Furthermore, this can speed up the procedure and bring down the cost of developing new software. Additionally, it suggests that the IoT system design may be divided into functional units and made modularity with a high-level knowledge of each layer, as shown in Figure 3.

3.1 Cloud server with internet gateway

All gadgets linked to the system submit their information to the software management cloud server, which then delivers it to the Internet gateway. An internet network device typically consists of a microcontroller that can process huge data streams, has the computing ability to analyse the data, and is connected to the internet so that the data may be sent to databases for further processing and storage. An IoT program's internet gateway component is often a portable device with an integrated LAN and/or area network connection. The device in question is always on and connected by the mains. Data packets are often kept locally for backup purposes and transferred to the server on a regular basis. The sensor network is configured using the instructions that are also received from the server by this device.

3.2 Asymmetric password

Secret key techniques, also known as asymmetric key methodologies, use distinct keys for cipher – text decoding and plaintext encrypting. A secret key and a session key make up each of the two keys. The sender, who is known to everyone, is encrypted using the public key, and the confidential recipient is decrypted using the private key. One of the primary benefits of asymmetric ciphers is that they do not share keys as symmetric ciphers do. Asymmetric encryption's primary drawbacks, however, are that it uses too much energy and is slower than symmetric encryption. Elliptic curve cryptography (ECC) and Rivest-Shamir-Adleman (RSA) are two common asymmetric key methods used in cloud technology, as seen in Figure 4.

3.3 Wireless IoT techniques

Since wireless communication is easy to install and can be deployed in a variety of ways, it has been extensively employed in the IoT. Wireless LANs (WLANs), wireless data networks (WPANs), and low power wireless connections are the three types of wireless networks (LPWANs). Figures 4 and 5 gives an overview and comparison of many widely used wireless approaches.

Figure 4 Schematic representation of asymmetric encryption (see online version for colours)

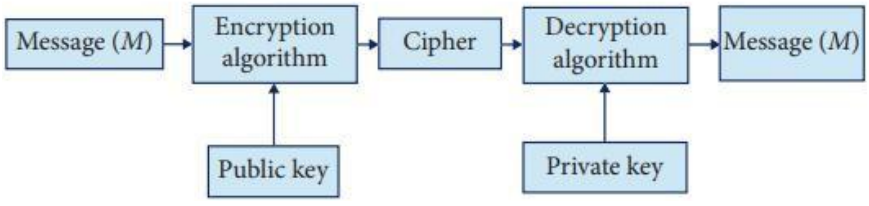
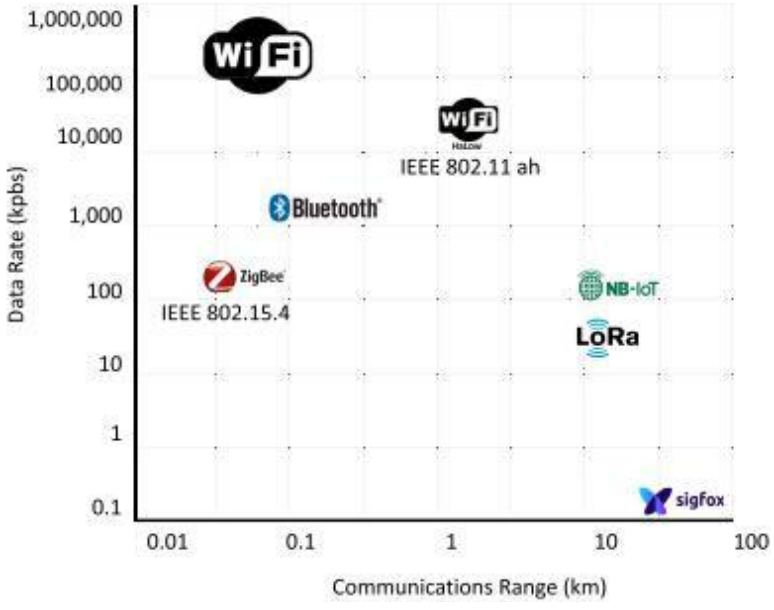


Figure 5 Internet wireless technologies (see online version for colours)



For instance, Wi-Fi, which is often used in computers and desktops, has a greater data throughput of about 100 Mbps but consumes a lot of energy. On the other side, LoRa, which is appropriate for sensor nodes, could only reach a speed of up to 50 kbps and could run for years on backup. This publication also uses the same taxonomy. Due to the fact that each wireless technology is created and optimised for a specific purpose, each has a unique communication range, maximum throughput, and energy consumption.

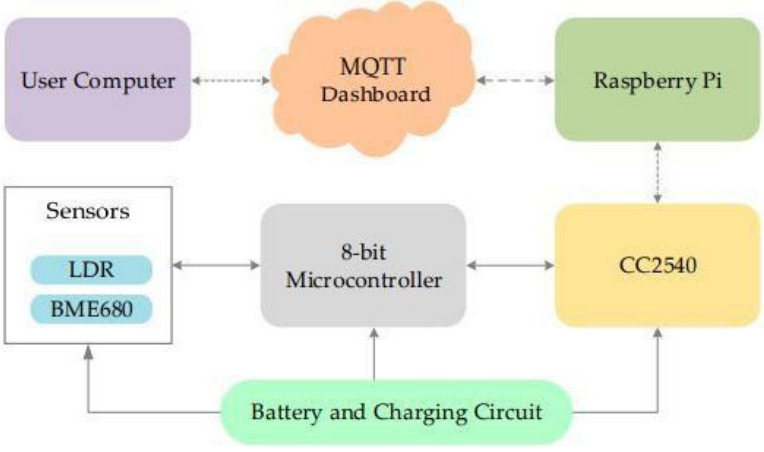
3.4 Sensors and actuators

An IoT system seeks to acquire, gather, and analyse data from the real environment at this level (the sensing layer). There are many attacks and risks that are particular to this layer; for instance, all WSN-specific risks and assaults are also included in the cyberattacks on IoT since the moment a compromised sensor node connected to IoT, the whole network becomes unreliable. The security of an entire system that spans the number of different technologies, transportation layer, and application server must also be considered as part of IoT security framework.

3.5 Indoor environmental monitoring

Monitoring the indoor environment is necessary to provide a secure working and living space. Inside this version of the LiB IoT network, as shown in Figure 7, heat, humidity, barometric pressure, and gas were monitored using the BME 680 sensor from Adafruit Companies in New York, NY, USA. Ambient illumination in the bedrooms was monitored using a light-sensitive diode. The BME 680 is a single, low wattage detector for measuring interior areas. The integrated sensor decreases latency, energy usage, and overall system performance since it monitors all three parameters. The detector interacts via the SPI protocol, has the ability to identify airborne contaminants, and provides a one-point resolution quantifiable value of the indoor air quality with a range of 0–500 points.

Figure 6 Tracking of indoor environmental systems network infrastructure (see online version for colours)



3.6 Heavy encryption and forward privacy

API for SSL transportation utilise Apple's secure API to make network connections utilising the most latest iterations of secure shell, network access securities, data transmission transport layer security encrypting protocols and helped algorithms. Now that iOS 10 and macOS 10.12 have been released, the RC4 cipher suite is deactivated by default. Additionally, Apple suggests that you upgrade your infrastructure so that they use certificates that have been signed using the SHA-2 cryptographic technique. Encryption-based signatures to validate the legality of your Mac software while making it available outside of the Mac App Store, use programmer ID-based cryptographic signing. Support for smart cards in the CryptoTokenKit. The CryptoTokenKit application makes it very simple to use contactless cards and other cryptographic devices in macOS. Microsoft refers to the encryption API: next generation as the CryptoAPI's long-term replacement on their website. It was designed with several extensible layers and encryption-independent behaviour. Some of its traits are listed below: the document makes reference to agile cryptography, authentication and compliance, suite B entry, generational sustain, rootkits support, inspection, and replacement random numbers.

4 Result and discussion

In this paper, we take into account a system model in which our purpose is to map the AES cryptographic arrangement to heterogeneous IoT devices in a very way that the transmission rate of the system is maximised while simultaneously minimising the lot of tools used. The throughput results with various weight configurations and varying numbers of users are shown in Figure 7.

Figure 7 Statistics of the average throughput using various weight ratios and device counts (see online version for colours)

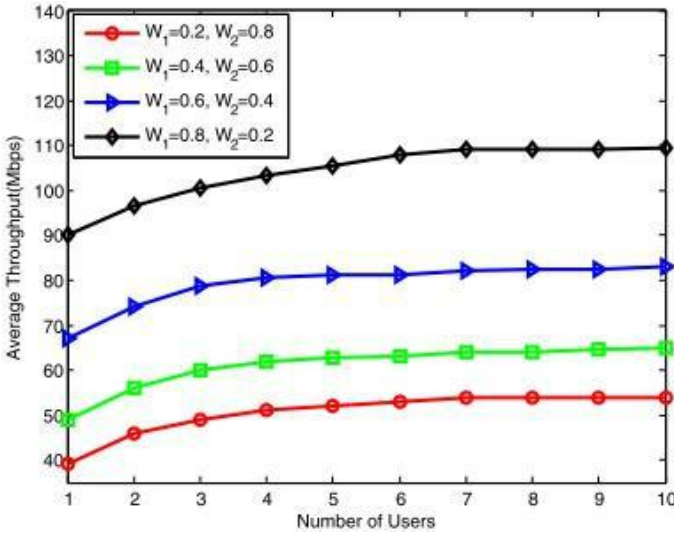
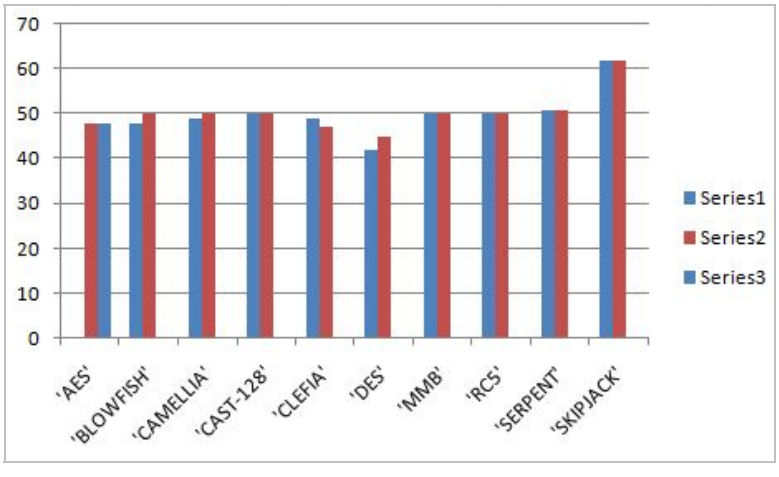


Figure 8 Avalanche impact results for all methods evaluated after fixing plaintext (see online version for colours)



We use a balanced function provided for this purpose. Through our suggested adaptive framework mentioned in section, combinations of various weights are applied to the

performance and resource variables in this equation to identify the strategies that provide the greatest outcomes. There are other studies carried out where the masses of the throughput and capabilities of the devices are also modified along with the quantity of end users (i.e., IoT devices). Finding the throughput/resource trade-off that produces the greatest overall performance is the major goal of this variant.

Super intelligent systems have been using info about farms to get their observations. While these may be the only information that supports a portion of a process in the college of agriculture, it is important to note that these data are significant. On the other side, Figure 8 shows which methods were improved by what percentage whenever the plaintext was set.

5 Conclusions

It is anticipated that IoT will integrate cutting-edge technologies of interaction, networking, cloud services, sensing and motion, and will pave the way for ground-breaking technologies in various of fields. These revolutionary applications will have an impact on many facets of people's lives and will bring about a great deal of convenience. Nevertheless, due to the vast number of interconnected devices that may be susceptible to attack, the IoT poses very significant dangers in terms of privacy, security, and overall governance. The next thing that we do is present an adaptable framework that takes into account the varied nature of IoT devices as well as measurements of various implementation approaches. The adaptive function applies a modified version of a bipartite matching graph in order to map the AES implementation strategies to the IoT devices. During the mapping process, the primary goal is to maximise the throughput of the IoT-based system while making the fewest demands on its resources. The Hungarian algorithm is being used to optimise this mapping procedure. We do a large number of experiments utilising the framework that was suggested. The outcomes of the suggested framework are compared with those of the randomised and greedy method. This comparison is undertaken. According to the analysis of the obtained data, the proposed framework delivers, on average, results that are 11% and 17% better in terms of average throughput and 3% and 13% better in terms of resource usage when especially in comparison to the random and selfish approaches, respectively. AES may be implemented in software on edge devices with a large amount of processing capabilities, leaving opportunity for application firmware. Therefore, quick implementation times may be achieved while maintaining a sufficient level of security using lightweight cryptographic approaches like SEA and XTEA. Given that these techniques are more effective, this would be the case. The usefulness of these techniques has been determined via testing on a number of different IoT applications. In general, the suggested LiB technique for solving a modularity approach to the design of IoT applications in order to meet the issues that are associated with implementing a solution that is flexible, reliable, and accessible regardless of environment. These challenges may be broken down into many categories. In a head-to-head comparison with all of the methods, our modified (proposed) version fared better than the other strategies when the key was set. When the clear text was repaired, the modified version performed best than the other techniques. In this research, the avalanche effect was increased to 60% of the algorithms that were evaluated when the key was maintained and to 70% when the content was fixed.

References

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. (2015) 'Internet of things: a survey on enabling technologies, protocols, and applications', *IEEE Commun. Surveys Tuts.*, 4th quarter, Vol. 17, No. 4, pp.2347–2376.

Appel, M., Bossert, A., Cooper, S., Kußmaul, T., Löffler, J., Pauer, C. and Wiesmaier, A. (2016) *Block Ciphers for the IoT – SIMON, SPECK, KATAN, LED, TEA, PRESENT, and SEA Compared* [online] https://download.hrz.tu-darmstadt.de/pub/FB20/Dekanat/Publikationen/CDC/2016-09-05_TR_SimonSpeckKatanLedTeaPresentSea.pdf (accessed 28 May 2019).

Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B. and Wingers, L. (2013) 'The SIMON and SPECK families of lightweight block ciphers', *IACR Cryptol.*, ePrint Arch., p.404.

Bogdanov, A., Knudsen, L., Leander, G., Paar, C., Poschmann, A., Robshaw, M., Seurin, Y. and Vikkelsoe, C. (2007) 'PRESENT: an ultra-lightweight block cipher', *Lect. Notes Comput. Sci.*, Vol. 4727, pp.450–466.

Burg, A., Chattopadhyay, A. and Lam, K-Y. (2018) 'Wireless communication and security issues for cyber-physical systems and the internet-of-things', *Proc. IEEE*, January, Vol. 106, No. 1, pp.38–60.

Eisenbarth, T., Gong, Z., Guneysu, T., Heyse, S., Indesteege, S., Kerckhof, S., Koeune, F., Nad, T., Plos, T., Regazzoni, F. et al. (2012) 'Compact implementation and performance evaluation of block ciphers in ATtiny devices', in *Proceedings of the 5th International Conference on Cryptology in Africa*, Ifrance, Morocco, 10–12 July, pp.172–187.

Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. (2013) 'Internet of /ings (IoT): a vision, architectural elements, and future directions', *Future Generation Computer Systems*, Vol. 29, No. 7, pp.1645–1660.

Hasan, M.K., Ahmed, M.M., Hashim, A.H.A., Razzaque, A., Islam, S. and Pandey, B. (2020) 'A novel artificial intelligence based timing synchronization scheme for smart grid applications', *Wireless Personal Communications*, Vol. 114, No. 3, pp.1–18.

Kamil, S. (2018) 'Challenges in multi-layer data security for video steganography revisited', *Asia-Pacific Journal of Information Technology and Multimedia*, Vol. 7, No. 2, pp.53–62.

Mahajan, P. and Sachdeva, A. (2013) 'A study of Encryption algorithms AES, DES and RSA for security', *Glob. J. Comput. Sci. Technol.*, Vol. 13 [online] https://computerresearch.org/index.php/computer/article/view/272 (accessed 27 May 2019).

Majid, M.A. and Ariffin, K.A.Z. (2019) 'Success factors for cyber security operation centre (SOC) establishment', in *Proceedings of the 1st International Conference on Informatics, Engineering, Science and Technology*, INCITEST, Bandung, Indonesia, July.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J. and Aharon, D. (2015) *The Internet of Things: Mapping the Value Beyond the Hype*, McKinsey Global Institute, San Francisco, CA, USA.

Pérez, J.M.X., León, A.L., de la Peña, J.M.L.O. and Hernández Terrazas, R.O. (2012) 'Real time stereo vision with a modified census transform in FPGA', in *Proceedings of the IEEE International Conference on Electronics, Robotics and Automotive Mechanics Conference (CERMA)*, DOI: 10.119/CERMA.2012.23 (accessed 15 January 2018).

Shelby, Z., Hartke, K. and Bormann, C. (2014) 'The constrained application protocol (CoAP)', *Internet Engineering Task Force*, June, pp.1–110, ISSN: 2070-1721.

Shi, L., Yuan, J., Yu, S. and Li, M. (2013) 'ASK-BAN: authenticated secret key extraction utilizing channel characteristics for body area networks', in *Proc. 6th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, pp.155–166.

Shi, L., Yuan, J., Yu, S. and Li, M. (2015) 'MASK-BAN: movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks', *IEEE Internet Things J.*, February, Vol. 2, No. 1, pp.52–62.

Singh, D., Tripathi, G. and Jara, A.J. (2014) 'A survey of internet-of-things: future vision, architecture, challenges and services', in *Proc. IEEE World Forum on Internet of Things*, pp.287–292.

Xiao, Y., Chen, H., Sun, B., Wang, R. and Sethi, S. (2006) 'MAC security and security overhead analysis in the IEEE 802.15.4 wireless sensor networks', *EURASIP J. Wirel. Commun. Netw.*, December, Vol. 81, pp.1–2.