Dynamic Lightweight Mechanism for Security and Performance in Internet of Things

https://doi.org/10.3991/ijim.v16i10.30085

Sinan Adnan Diwan(✉)
College of Computer Sciences and Information Technology, Wasit University, Wasit, Iraq
sdiwan@uowasit.edu.iq

Abstract—Communication between machines has become commonplace in recent years, and the Internet of Things (IoT) is gaining notoriety. Congestion control is a prevalent issue in the transportation system, and GPS devices, which drivers and traffic authorities alike utilise, are well-suited to the job. Traffic density is expanding at an alarming rate, making it impossible for drivers to see and handle all of the possible scenarios in a traffic area they are ready to enter. It's also becoming increasingly difficult to maintain security and integrity due to a growing number of assaults by hackers that send harmful code or bogus packets. There are a few new technologies that have yet to be put into practise under the Internet of Things umbrella, including ubiquitous computing (IoT).

Keywords—Internet of Things, IoT, Security and Performance in IoT

1 Introduction

Kevin Ashton coined the term "Internet of Things" in 1999. The widespread use of IoT is due to the widespread availability of high-performance wireless technology. The Internet of Things relies on RFID tags and sensors as its foundational components. A software-based programme may be used to monitor RFID tags implanted in real-world equipment and objects. The RFID readers may be used to find, read, and detect the RFID implanted items. RFID can communicate over long distances because to the integration of extremely small, micro-sized transmitting and receiving chips [1–3].

According to Forbes.com, the Internet of Things industry is expected to reach $267 billion by 2020. Gartner's research shows that in 2017 roughly 8.4 billion things and 273 billion dollars in investment will be interconnected. This year's implementation of 8.4 billion items is a 31% increase over 2016.

The following are some of the most important IoT uses [4–9]:

- Cities with Smart Infrastructure
- Smart Shopping Centers
- In addition, the "Smart Grid"
- Smart farming and agriculture
- Vehicle-to-vehicle Internet (IoV)
- Autonomous Vehicles That Are Always Connected

- Infrastructural Connectivity
- Wearable Gadgets : Devices That Can Be Worn
- Smart House
- Offices with cutting-edge technology
- Software Defined Communications
- Intuitive Distribution Network
- Innovative Medical Technology, Including Intelligent Ambulances
- Internet of Things (IoT)
- Energy Conservation
- and many others

2 Problem

As you can see, Intelligent Transportation Systems are being used in a variety of ways all around the world. Projection and display of shifting speed restriction information on intelligent traffic control lights Disobeying traffic signals and warnings, the Auto-Detection of Number Plate System The Use of Speed-Sensing Cameras. Systems for Preventing and Detecting Collisions. The use of vehicle-based emergency alert systems [10].

Internet of Things technology trends are seen in Figure 1 as the Internet of Things booms across the board due to technical advancements.

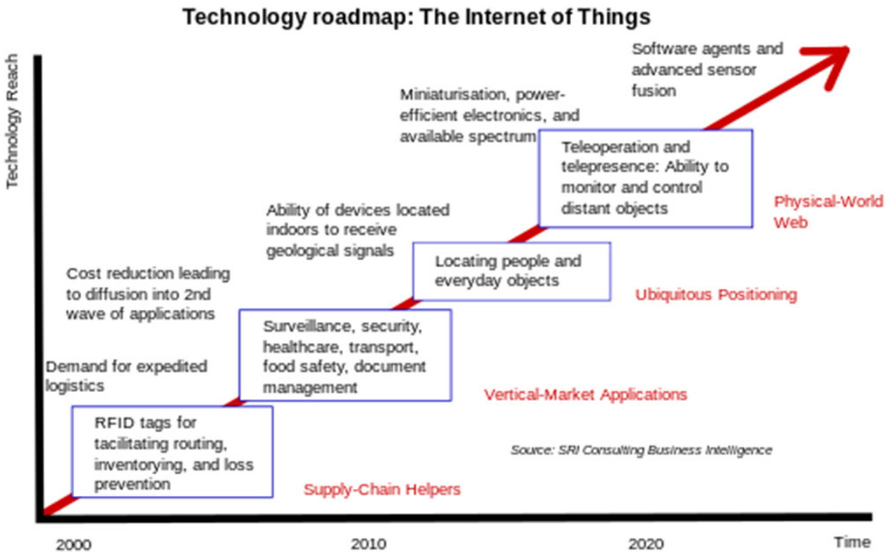

Technology roadmap: The Internet of Things
Technology Reach
Software agents and advanced sensor fusion
Miniaturisation, power-efficient electronics, and available spectrum
Teleoperation and telepresence: Ability to monitor and control distant objects
Physical-World Web
Ability of devices located indoors to receive geological signals
Locating people and everyday objects
Ubiquitous Positioning
Cost reduction leading to diffusion into 2nd wave of applications
Surveillance, security, healthcare, transport, food safety, document management
Vertical-Market Applications
Demand for expedited logistics
RFID tags for facilitating routing, inventorying, and loss prevention
Supply-Chain Helpers
Source: SRI Consulting Business Intelligence
2000
2010
2020
Time

Fig. 1. Technology roadmap with IoT

Because the Internet of Things is based on the premise that everything can be linked together, interconnectivity is a critical characteristic (despite the traffic going through different networks) [11].

3 IoT based virtual infrastructure

At various levels of the VANET's defences, several assault types are employed to exert influence and do harm. Vehicle nodes and the infrastructure they are connected to are the most important parts of the VANET. Using malicious packets and signals, attackers may be able to harm and control the vehicle network, causing the entire infrastructure to be essentially destroyed. Attacks that affect the entire network score high on the list of threats. There are a lot of assaults on the vehicular networks that are often used to control and damage them [12].

A denial-of-service (DoS) attack prevents a node or malicious packet from accessing the network. One of the most common assaults against VANET's network layer is denial of service (DoS) [13].

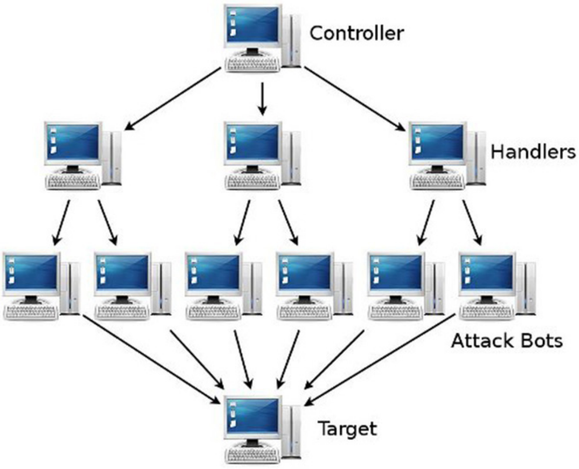


Fig. 2. DDoS attack in IoT based environment

A distributed denial-of-service (DDOS) assault is particularly harmful in a VANET because of the dispersed nature of the mechanism involved. To carry off this attack successfully, the rogue node or attacker must operate from a variety of distinct places. The analytics 3 indicates that legitimate or authentic systems are unable to communicate in the network due to multidirectional congestion or blockage [14].

Sybil Attack-The vehicular network's network layer is severely affected by the Sybil attack. The identity of the source is modified in this assault. Fake or fabricated identities are used by the malicious node to seem as though it is the source node. One node attacks another by replicating itself and forcing them to leave or move quickly from the road, which is known as a Sybil assault. Resource testing, which assumes that vehicles have limited resources, can be used to identify these assaults. It is possible to protect against the Sybil attack by utilising public key cryptography to authenticate automobiles [15].

In a node imitation attack, communications are sent via an impersonated node with a different identity. So an attacker can transmit harmful or incorrect signals to any node that changes or hides its identity [16].

Message Level – In this attack, the alteration is done in the message received and then retransmitted to other adjacent nodes or cars. Message Level – Damage to the network infrastructure and traffic might occur in this manner, as well. Retransmitting the original message with the new wording such as "Road Free Ahead, Move Fast" is an example of how this technique might be used. Using this method, the network congestion might worsen and lead to an accident in the near future [17].

The modernisation of transportation is currently a major factor in a country's growth and development. Innovative transportation systems have been made possible by advancements in communication and networking technology, as well as vehicle positioning technologies. In the transportation of dangerous commodities, logistics, armoured car, and other specific industries, these three primary approaches for autonomous location-sensing are frequently utilised.

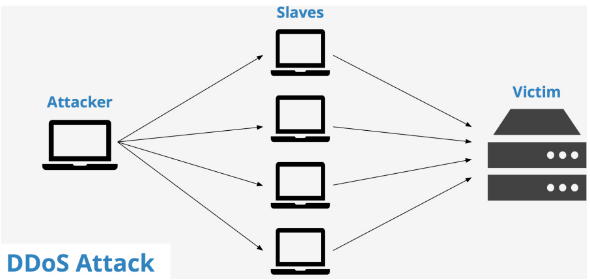


Fig. 3. DDoS in internet of vehicles

4 Goals with analysis with proximity of object

It is possible to categorise the Internet of Things into four distinct layers: perception, network, service, and application. It is the network layer that allows the many Internet-connected devices to communicate with one another, while the service layer provides services to the application or end user for further cognitive processing. We may expect a wide range of new applications and services as a result of this powerful vision of the Internet of Things in Intelligent Transportation Systems (ITS). However, the Internet of Things has other difficulties that must be overcome, including real-time traffic management, seamless connection, vehicle position prediction, security and privacy, interoperability, and communications.

- Intelligent transportation, linked cars, and the Internet of Things are the next generation of transportation systems [18, 19].
- a system that uses the Internet of Things to keep tabs on moving vehicles in real time
- Applications and services for real-time traffic control based on Internet of Things architecture for a distributed intelligent transportation system.
- Sensors and embedded systems for smart transportation.
- The use of wireless sensors in intelligent transportation systems.
- Advanced sensing technologies are used to forecast a vehicle's position.

- Fleet management and safety may be improved with the use of peer-to-peer data sharing.
- For location-based services, we've integrated transportation and sensors.

Using wireless sensor networks, information may be exchanged between an application platform and one or more sensors. This conversation is conducted entirely over the air [20].

The Internet of Things (IoT) and RFID have several applications in a variety of industries, as indicated. Temperature, humidity, vibration, motion, light, pressure, and altitude are just a few of the many uses for sensors. Big data from sensors will necessitate the development of new applications by companies. Radio-frequency identification (RFID) tags are becoming increasingly widely used because of their reduced costs and more advanced capabilities. More than only the tag itself, RFID's cost has decreased considerably. A genuine cost-per-use calculation includes the cost of software programs and their implementation. It's time for businesses to reassess their RFID strategies in light of the new value they're getting from decreased tag prices combined with better capabilities [21].

5 Ubiquitous sensor network

Y.2221 describes the USN as a theoretical system built on current physical systems that makes use of felt information and provides learning services to everyone, everywhere, and at any time and location where the data is generated via establishing awareness.

The term "physical systems" here refers to WSNs of various types, as well as wired sensor systems and radio frequency identification (RFID).

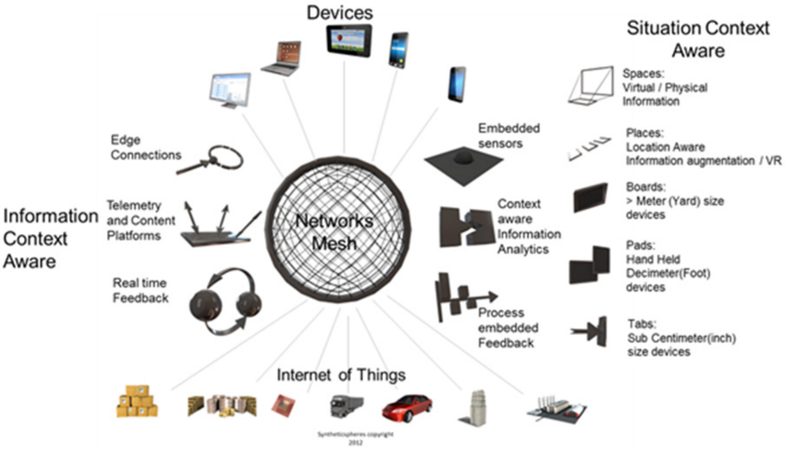

Devices
Situation Context Aware
Spaces: Virtual / Physical Information
Places: Location Aware Information augmentation / VR
Boards: > Meter (Yard) size devices
Pads: Hand Held Decimeter(Foot) devices
Tabs: Sub Centimeter(inch) size devices
Embedded sensors
Context aware Information Analytics
Process embedded Feedback
Edge Connections
Information Context Aware
Telemetry and Content Platforms
Real time Feedback
Networks Mesh
Internet of Things
Syntheticspheres copyright 2012

Fig. 4. Ubiquitous environment

6 Components in IoT environment and sensors

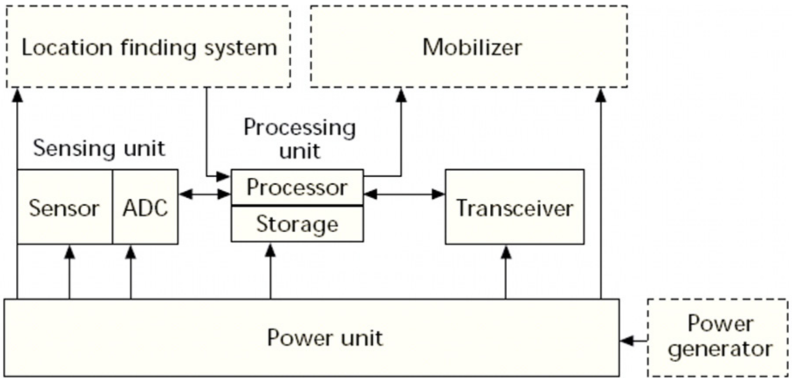


Fig. 5. Components with IoT sensors

6.1 RPL (Routing Protocol over Low Power and Lossy Networks)

Routing Protocol for Low-Power and Lossy Networks (RPL) is an open standard developed by the Internet Engineering Task Force (IETF) for IoT networks based on IPv6. The Internet of Things has adopted it as an approved routing layering pattern (IoT). RPL has contributed to the expansion of correspondences in the field of little, inserted, organising devices by providing, alongside various measures, gauge engineering for the Internet of Things.

Due to the low-power and lossy radio interfaces, the battery-provided hubs, the multi-bounce work topologies, and the subsequent topology modifications as a result of mobility, 6LoWPAN routing challenges are particularly difficult. IPv6 conduct and 6LoWPAN systems must be taken into account in every successful arrangement. The IETF Routing over Low Power and Lossy (ROLL) systems working gathering generated a persuasive arrangement. As a result of utilising an inclination-based strategy, RPL, the primary IPv6 Routing Protocol for Low Power and Lossy Networks (LLNs), was suggested [22].

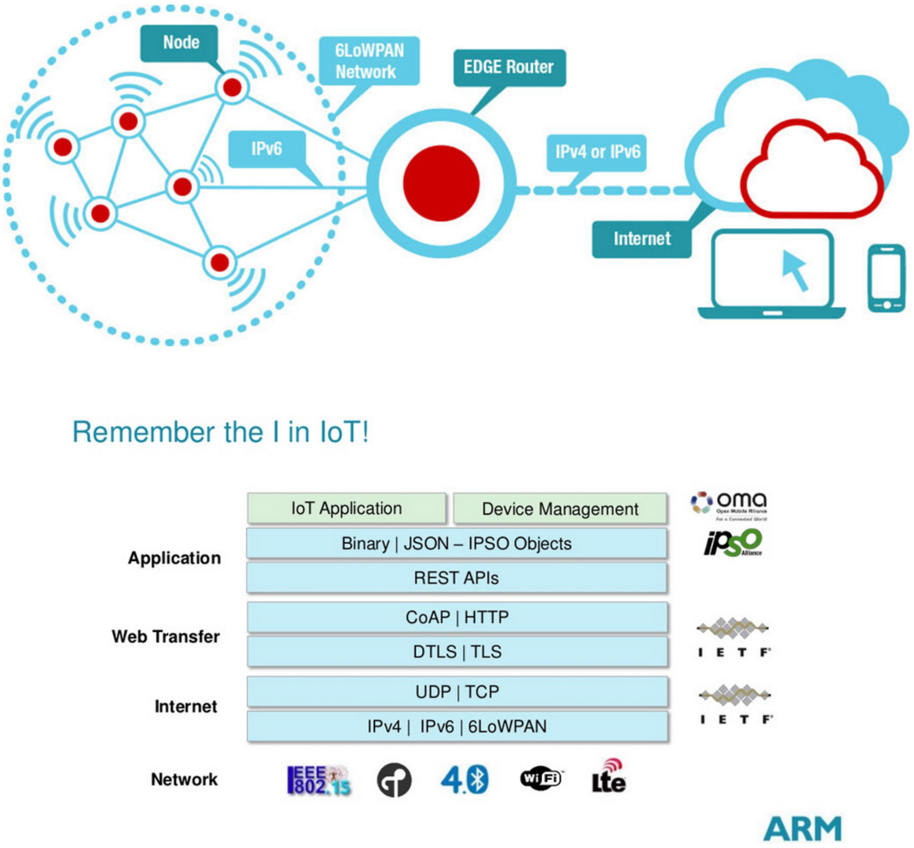


Fig. 6. LowPAN scenario

7 Methodology and projected approach

Because this library makes use of sensor nodes or motes, it is necessary to implement SHA in a Cooja-based environment. Because of this, SHA cannot be used with Cooja-based frameworks. Each SHA variation is tested in a variety of sensor notes in an IoT context to see how well it performs in comparison to the others. Machine-to-machine communication in an IoT network requires security and integrity to be addressed. The suggested method uses Cooja Simulation to develop SHA variations on the Contiki Platform for IoT. Security and integrity are ensured via Secured Hash

Approach, a key mechanism. The primary motivation for working in this area is the lack of SHA implementation on Cooja in research implementations. A family of cryptographic algorithms known as SHA is utilised for security and dynamic encryption, and these algorithms create keys of varying sizes, hashes, and lengths, which may be used for network security and overall integrity.

The main standards of SHA with related bit stream size includes

- SHA-1
  - 160
- SHA-0
  - 160
- SHA-2
  - 384
  - 256
  - 512
- SHA-3
  - 256
  - 224
  - 384
  - 512

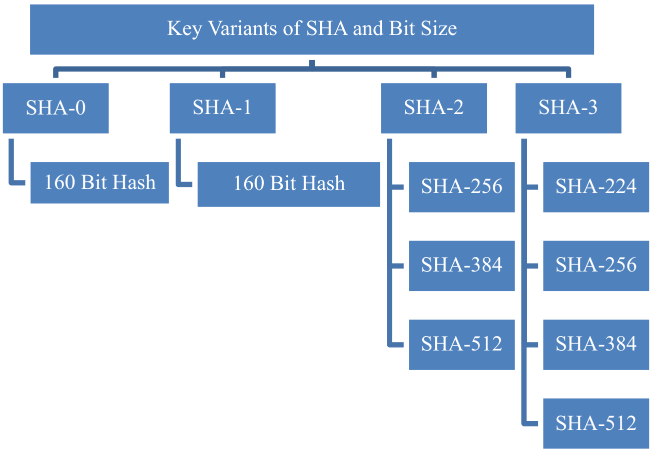


Fig. 7. Variants with cryptography approach

8 Results and performance analytics

The implementation patterns and simulation scenarios are generated using open source platforms and the effective results are fetched.

Table 1. Analytics on approaches

Variant	Block Size	Rounds	Output Size
SHA-0	512	80	160
SHA-1	512	80	160
SHA2-224	512	64	224
SHA2-256	512	64	256
SHA2-384	1024	80	384
SHA3-224	1152	24	224
SHA3-256	1088	24	256
SHA3-384	832	24	384
SHA3-512	576	24	512

Routing over Low Power and Lossy Networks (RPL) is a Distance Vector IPV6 routing protocol for loss-less networks, and this study focuses on the implementation of SHA and its variations.

The RPL devices are linked together using a topology known as DODAG, which combines mesh and tree topologies. Despite the fact that methods like

- Global and Local Repair can prevent assaults on IoT network resources by RPL.
- Fast-paced DODAG construction and management.
- Dynamic routing metrics and limitations can be supported.
- Detection and avoidance of loops.
- Timer Control.

In spite of the RPL's security procedures, the LLN network is particularly vulnerable to assaults because to its resource limits, lack of infrastructure, poor physical security, fluctuating topology and unreliable connectivity. Attacks on resources, topology, or traffic are all possibilities. When a malicious node causes other nodes to create a network overload, there are two basic forms of indirect attacks on resources. It consists of Malicious nodes that intentionally raise the rank value of an RPL node can employ this technique to create network loops. Version Number Attacks: DIO messages have a version number field. When a DIO communication is transmitted to a neighbour node, the attacker has the ability to corrupt this field. Unnecessary rebuilding of the whole DODAG occurs as a result of such an attack. Due to the various loops that can be created by this type of hacking, data packets may be lost. Graph re-building increases control message overhead and depletes nodes' resources, further clogging the network. To prevent hacked nodes from masquerading as the root and providing an illegitimately high Version Number, there is an authentication technique called VeRA (Version Number and Rank Authentication). In order to authenticate users, the system employs hashing techniques [23]. If this is the case, a node may readily determine if the root node or another rogue node has updated the Version Number. Therefore, it is imperative that the

IoT infrastructure be designed and deployed with algorithms for improved security and dynamic key exchange in mind. Higher levels of integrity and security in IoT may be imposed using multi-level hybrid key-based algorithms. By implementing multi-level hybrid key exchange utilising hash functions and self-created algorithms, the communication between IoT devices may be made safe and trustworthy. Because of this, the issue is phrased as.

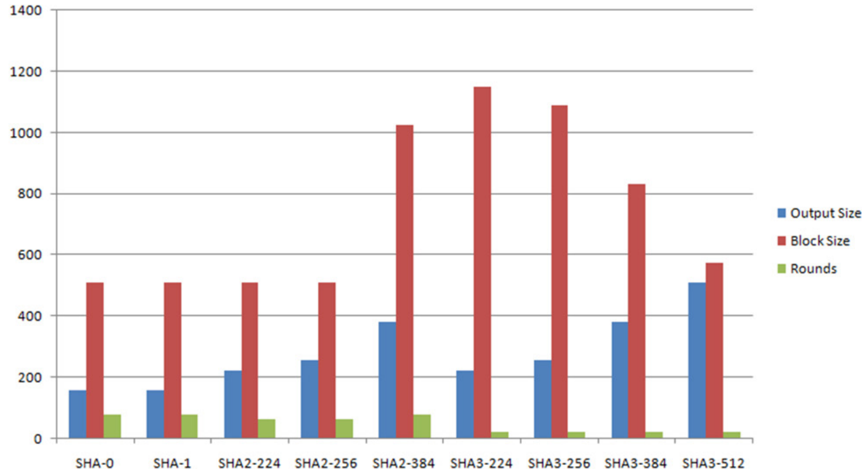


Fig. 8. Evaluation patterns of SHA

8.1 Simulation environment

SHA stands for Secure Hashing Algorithms, a group of cryptographic procedures aimed at safeguarding data. A hash function is an algorithm that uses bitwise operations, modular additions, and compression functions to change the data into a new form. Afterward, the hash function generates a string of fixed length that is completely unrelated to the original. Once the data has been turned into a hash value, it's very hard to get it back to its original form because these methods are one-way functions. SHA-1, SHA-2, and SHA-5 are some of the algorithms of interest, each of which was devised in response to hacker attempts. For example, the publicly known flaws in SHA-0 have rendered it outdated. As the server side just has to maintain track of a single user's hash value, rather than the actual password, SHA is frequently used for password encrypting. Hackers will only find hashed functions rather than passwords in a database breach, therefore if an attacker attempts to use the hashed value as a password, it will be converted into another string and denied access by the hash function. Additionally, the avalanche effect occurs with SHA, meaning that even little changes to the encrypted string can have a significant impact on the hash result. Hash values do not reveal any information about the input string, such as its original length, because of this. When data is altered even little by an attacker, the hash value of the modified file will be different from the original file's value, and the alteration will be easily detectable. SHAs are also used to identify tampering of data by attackers.

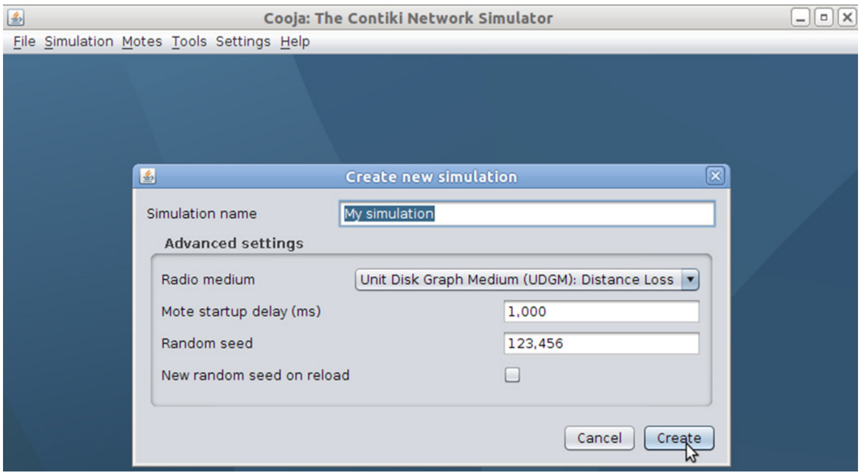
As resources become more scarce, it is imperative that the security and integrity of an IoT network, as well as its responsiveness and turn-around time, be not jeopardised. As a result, the proposed work aims to improve performance, turnaround time, and security and integrity in a resource-constrained context.

1. To use the Contiki-Cooja simulator to examine IoT implementation perspectives.
2. To use the SHA algorithm in the Cooja simulator on the Contiki Platform for IoT.
3. To examine the IoT's performance across several factors using various SHA algorithm versions

Integrity; Latency; Resource Optimization; Security

The Secured Hash Algorithm (SHA) versions are implemented in the IoT context in this study. Multiple parameters and resource optimization considerations in the Internet of Things Scenario are impacted by SHA-1, SHA-2-256, and SHA-3-256, the most important versions in this research.

8.2 Implementation scenario and simulation


Cooja: The Contiki Network Simulator
File Simulation Motes Tools Settings Help
Create new simulation
Advanced settings
Cancel
Create

Simulation name: My simulation

Radio medium: Unit Disk Graph Medium (UDGM): Distance Loss

Mote startup delay (ms): 1,000

Random seed: 123,456

New random seed on reload □

Fig. 9. Setup of Cooja simulation on IoT

Importing RFID tags, sensor nodes, and other IoT-related wireless devices is necessary once the basic structure and working environment have been established. These are referred to as "motes" in the context of wireless networking and the Internet of Things. Cooja's motes may be configured to do a variety of tasks.

System ports allow physical motes to be attached for real-time interface. Cat, the back-end of Cooja, specifies every mote's basic attributes and programming APIs. These motes' C source code files can be modified and recompiled to produce new or desired results.

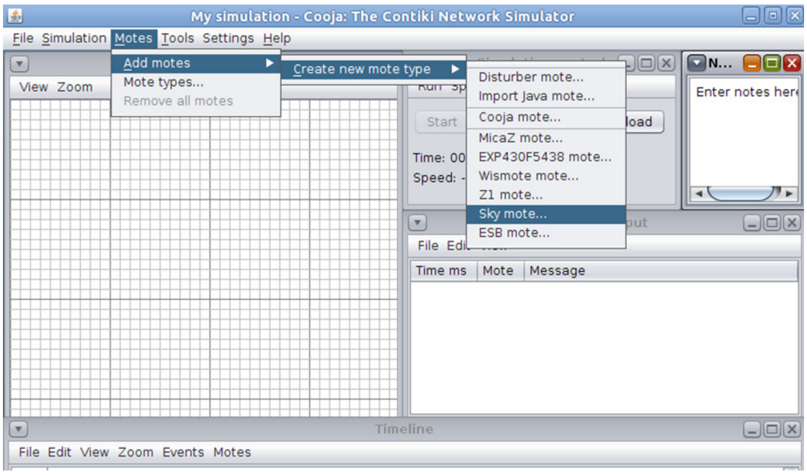
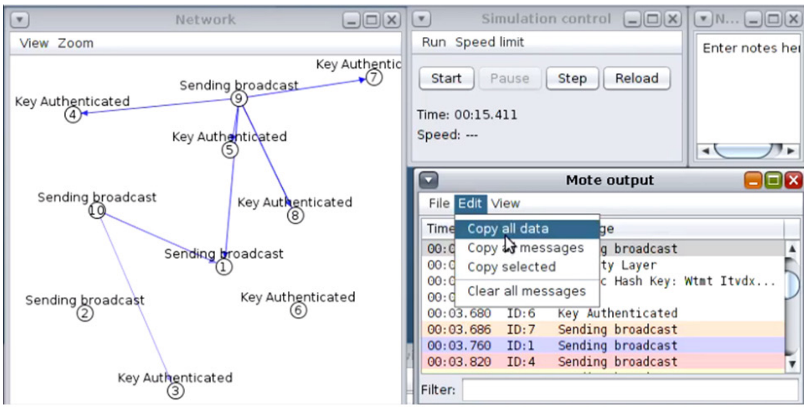
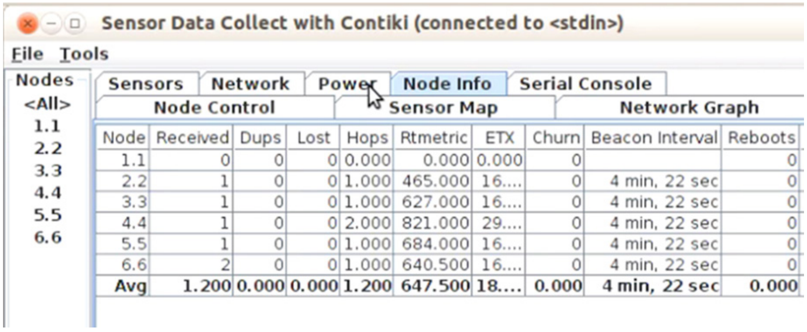


Fig. 10. Invoking RFID wireless motes



```
Time                   ge
00:0                   g broadcast
00:0                   ty Layer
00:0                   c Hash Key: Wtmt Itvdx...
00:0
00:03.680   ID:6    Key Authenticated
00:03.686   ID:7    Sending broadcast
00:03.760   ID:1    Sending broadcast
00:03.820   ID:4    Sending broadcast
```

Fig. 11. Implementation environment of approach



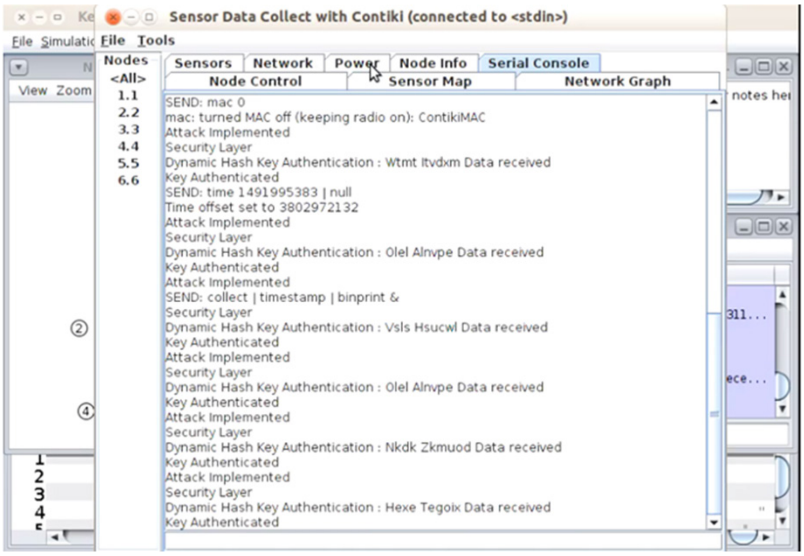
Node	Received	Dups	Lost	Hops	Rtmetric	ETX	Churn	Beacon Interval	Reboots
1.1	0	0	0	0.000	0.000	0.000	0		0
2.2	1	0	0	1.000	465.000	16....	0	4 min, 22 sec	0
3.3	1	0	0	1.000	627.000	16....	0	4 min, 22 sec	0
4.4	1	0	0	2.000	821.000	29....	0	4 min, 22 sec	0
5.5	1	0	0	1.000	684.000	16....	0	4 min, 22 sec	0
6.6	2	0	0	1.000	640.500	16....	0	4 min, 22 sec	0
Avg	1.200	0.000	0.000	1.200	647.500	18....	0.000	4 min, 22 sec	0.000

Fig. 12. Evaluation of logs of sensor nodes

Execution Scenario: 1 Number of Motes: 11 Source Mote: 3 Sink Motes: 6

Table 2. Execution scenario: 1

Algorithm	Power Consumption (mW)	Latency	Passes
SHA-1	0.81	0.54	81
SHA-2	0.92	0.38	62
SHA-3	0.78	0.20	26



```
SEND: mac 0
mac: turned MAC off (keeping radio on): ContikiMAC
Attack Implemented
Security Layer
Dynamic Hash Key Authentication : Wtmt Itvdxm Data received
Key Authenticated
SEND: time 1491995383 | null
Time offset set to 3802972132
Attack Implemented
Security Layer
Dynamic Hash Key Authentication : Olel Alnvpe Data received
Key Authenticated
Attack Implemented
SEND: collect | timestamp | binprint &
Security Layer
Dynamic Hash Key Authentication : Vsls Hsucwl Data received
Key Authenticated
Attack Implemented
Security Layer
Dynamic Hash Key Authentication : Olel Alnvpe Data received
Key Authenticated
Attack Implemented
Security Layer
Dynamic Hash Key Authentication : Nkdk Zkmuod Data received
Key Authenticated
Attack Implemented
Security Layer
Dynamic Hash Key Authentication : Hexe Tegoix Data received
Key Authenticated
```

Fig. 13. Dynamic hash generation using SHA

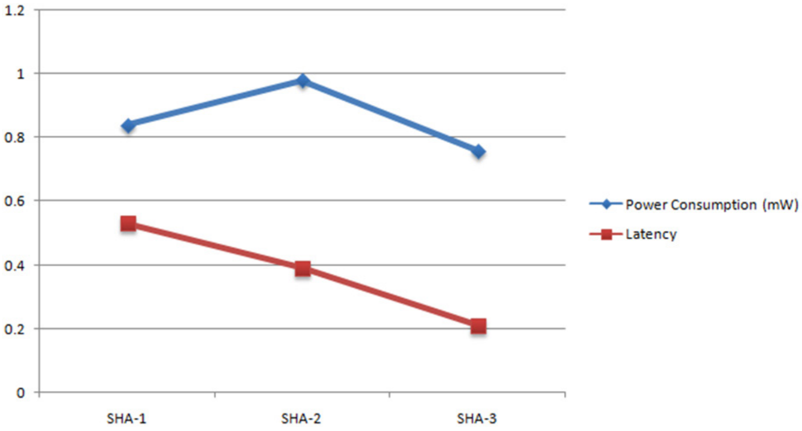


Fig. 14. Evaluation of power consumption and latency

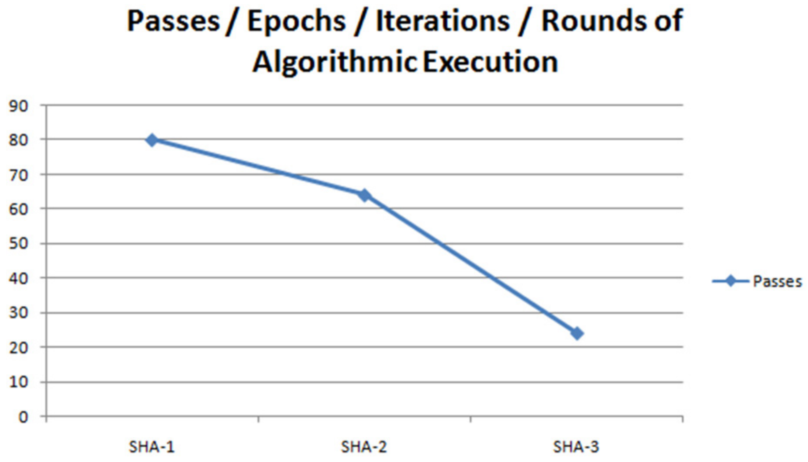


Fig. 15. Line graph evaluation of algorithmic rounds

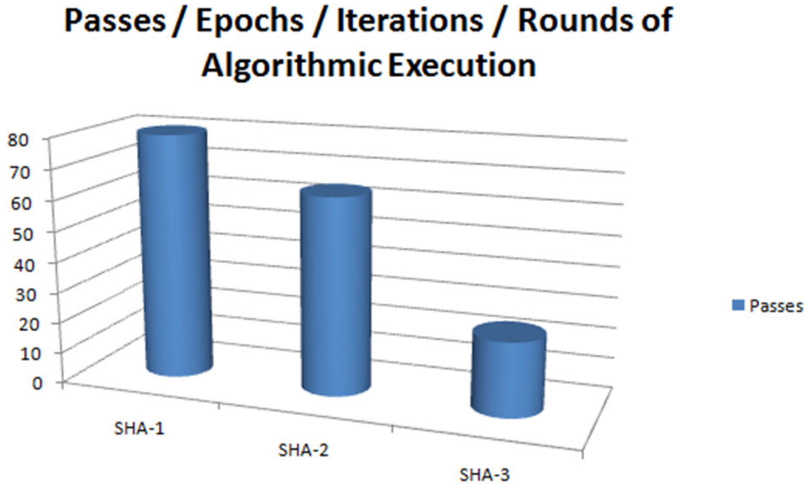


Fig. 16. Bar graph evaluation of rounds or epochs

Number of Motes: 22 Source Mote: 1 Sink Motes: 12

Table 3. Execution scenario: 2

Algorithm	Power Consumption (mW)	Latency	Passes
SHA-1	0.92	0.42	81
SHA-2	0.84	0.39	63
SHA-3	0.62	0.22	23

Increased security and efficiency in IoT networks may be achieved by implementing the hybrid key technique that has been developed. It is expected that SHA-based Key Exchange would increase the integrity of data transfer, as well as the overall efficiency of the system. SHA-3's overall performance is superior than that of SHA-1 and SHA-2. Because SHA-3 uses fewer rounds and is therefore more resource efficient, it also provides a better level of security while using less power.

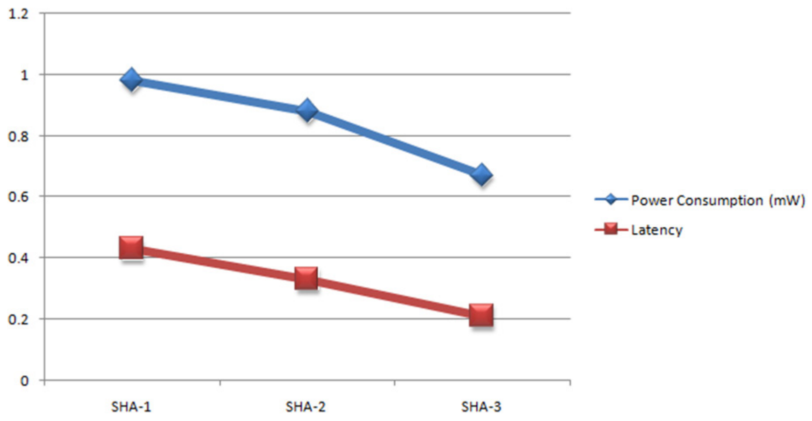


Fig. 17. Evaluation of power and latency with 12 motes

9 Conclusion

It seems like every day we read of a new way an unsecured IoT gadget has been hacked, making the Internet of Things (IoT) seem awful. It is only via the right application of encryption that the Internet of Things may become more secure. And it's not the kind of cryptography you'd make on your own, either. Many instances exist of do-it-yourselfers underestimating the time and effort required to construct a safe gadget, only to have their efforts reduced to nothing more than a game for a cybercriminal. And there's no excuse for not employing proven, standards-compliant cryptographic algorithms thanks to the abundance of encryption libraries available for practically any programming language. The internet of things relies heavily on encryption to protect its communication routes. The implementation of Transport Layer Security (TLS) in IoT-centric communication protocols like MQTT and AMQP ensures that all data passed over the network is unreadable by third parties. TLS is the natural successor to SSL, which was the long-time standard for web encryption (see HTTPS) but is now regarded unsafe. It is impossible for a third party to view or manipulate data exchanged through TLS. Secondary communication channels, such as those used for system maintenance or customer features, should also be encrypted in addition to the primary data connections. The default encryption for an IoT device's web portal (such as a printer's web interface) should be enabled by default. Anyone on the same network might steal login credentials and use them to pretend to be the person controlling these devices if this isn't done. Secure Shell should be used instead of insecure maintenance interfaces like telnet because of this (SSH). To paraphrase an old saw, the safest systems are those in which there is nothing to steal. You may do this by storing hashed passwords. A hash function is a type of cryptographic algorithm that takes an input and generates a collection of bits that is both unique and unchangeable. Reversing a good hash algorithm is next to impossible. You should be unable to reverse a password's hash to find out what the password was once it's been hashed. As a result of this, the hash may still be used to verify password submissions because the same input to a hashing function will get the same output or hash. MD5 (popular but no longer considered secure), SHA-256, and Blowfish are all examples of hashing functions. A rainbow table, or look-up table, is a common assault on hashing. This is a database that stores the hashed results of every possible (or at least frequent) text input. The result of a hash may be swiftly reverse-searched using this method. A rainbow table might easily be used to restore the original password hashes if a hacker obtained a list from a hacked system. It is possible to counteract this onslaught, though, by using a salt. Prior to hashing, the salt appends a random collection of data to the string. It is stored alongside the hash result, however the salt varies each hash so that no two hashes would have the same salt. If you're hashing passwords, the salt makes them so lengthy and unpredictable that rainbow tables are rendered worthless. Creating a rainbow table for every huge, random string is too time-consuming. There are two keys in private key cryptography: one public and one private. Only the public key can decrypt data encrypted using the private key, and vice versa. One machine can connect with the outside world or authenticate with remote machines if its private key is kept private. Several areas of IoT architecture benefit greatly from this specific piece of cryptographic technology. The first step is to verify the identity of a single IoT device. To post data upstream, an end node might need to connect to a central MQTT broker. Because of their length, private keys are very tough to brute force when a computer joins the network, replacing the common but unsafe global credential technique (which is where a machine is programmed to guess values). The verification of communications between devices is the second area in which private keys might aid with IoT. A private key would be used to encrypt a message (such as a firmware image) and then attach a hash or other integrity-checking method to the message. The recipient of the message uses the public key to decode the check, which reveals that it could only have been created by the person who possessed the private key in the initial instance.

10 References

[1] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight Cryptography: A Solution to Secure IoT," Wireless Personal Communications, vol. 112, no. 3, pp. 1947–1980, 2020. https://doi.org/10.1007/s11277-020-07134-3

[2] N. Hussien, I. Ajlan, M. M. Firdhous, and H. Salim, "Smart Shopping System with RFID Technology Based on Internet of Things," International Journal of Interactive Mobile Technologies, vol. 14, no. 4, pp. 17–29, 2020. https://doi.org/10.3991/ijim.v14i04.13511

[3] H. T. S. ALRikabi, A. H. M. Alaidi, and F. T. Abed, "Attendance System Design and Implementation Based on Radio Frequency Identification (RFID) and Arduino," Journal of Advanced Research in Dynamical Control Systems, vol. 10, no. SI4, pp. 1342–1347, 2018.

[4] M. A. F. Al-Husainy, B. Al-Shargabi, and S. Aljawarneh, "Lightweight Cryptography System for IoT Devices using DNA," Computers Electrical Engineering, vol. 95, p. 107418, 2021. https://doi.org/10.1016/j.compeleceng.2021.107418

[5] F. T. Abed, H. T. S. ALRikabi, and I. A. Ibrahim, "Efficient Energy of Smart Grid Education Models for Modern Electric Power System Engineering in Iraq," in IOP Conference Series: Materials Science and Engineering, 2020, vol. 870, no. 1, p. 012049: IOP Publishing. https://doi.org/10.1088/1757-899X/870/1/012049

[6] H. T. S. Alrikabi and N. Ali Jasim, "Design and Implementation of Smart City Applications Based on the Internet of Things," International Journal of Interactive Mobile Technologies (iJIM), vol. 15, no. 13, pp. 4–15, 2021. https://doi.org/10.3991/ijim.v15i13.22331

[7] O. H. Yahya, H. T. ALRikabi, R. a. M. Al_airaji, and M. Faezipour, "Using Internet of Things Application for Disposing of Solid Waste," International Journal of Interactive Mobile Technologies, vol. 14, no. 13, pp. 4–18, 2020.

[8] B. K. Mohammed, M. B. Mortatha, A. S. Abdalrada, "A Comprehensive System for Detection of Flammable and Toxic Gases using IoT," vol. 9, no. 2, pp. 702–711, 2021. https://doi.org/10.21533/pen.v9i2.1894

[9] H. T. Salim, I. A. Aljazaery, "Encryption of Color Image Based on DNA Strand and Exponential Factor," International Journal of Online and Biomedical Engineering (iJOE), vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28021

[10] B. Seok, J. C. S. Sicato, T. Erzhena, C. Xuan, Y. Pan, and J. H. Park, "Secure D2D Communication for 5G IoT Network Based on Lightweight Cryptography," Applied Sciences, vol. 10, no. 1, p. 217, 2020. https://doi.org/10.3390/app10010217

[11] I. Bhardwaj, A. Kumar, and M. Bansal, "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), 2017, pp. 504–509: IEEE. https://doi.org/10.1109/ISPCC.2017.8269731

[12] I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight Cryptography for Internet of Insecure Things: A Survey," in 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp. 0475–0481: IEEE. https://doi.org/10.1109/CCWC.2019.8666557

[13] 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. https://doi.org/10.1080/23742917.2017.1384917

[14] N. A. Gunathilake, W. J. Buchanan, and R. Asif, "Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications," in 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), 2019, pp. 707–710: IEEE. https://doi.org/10.1109/WF-IoT.2019.8767250

[15] S. Atiewi, A. Al-Rahayfeh, M. Almiani, S. Yussof, O. Alfandi, A. Abugabah, and Y. Jararweh, "Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography," IEEE Access, vol. 8, pp. 113498–113511, 2020.

[16] A. Fotovvat, G. M. Rahman, S. S. Vedaei, and K. A. Wahid, "Comparative Performance Analysis of Lightweight Cryptography Algorithms for IoT Sensor Nodes," IEEE Internet of Things Journal, vol. 8, no. 10, pp. 8279–8290, 2020.

[17] M. Khalifa, F. Algarni, M. A. Khan, A. Ullah, and K. Aloufi, "A Lightweight Cryptography (LWC) Framework to Secure Memory Heap in Internet of Things," Alexandria Engineering Journal, vol. 60, no. 1, pp. 1489–1497, 2021. https://doi.org/10.1016/j.aej.2020.11.003

[18] S. B. Sadkhan and A. O. Salman, "A Survey on Lightweight-Cryptography Status and Future Challenges," in 2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA), 2018, pp. 105–108: IEEE. https://doi.org/10.1109/ICASEA.2018.8370965

[19] H. Tauma and H. Alrikabi, “Enhanced Data Security of Communication System using Combined Encryption and Steganography,” International Journal of Interactive Mobile Technologies, vol. 15, no. 16, pp. 144–157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[20] T. K. Goyal, V. Sahula, and D. Kumawat, “Energy Efficient Lightweight Cryptography Algorithms for IoT Devices,” IETE Journal of Research, pp. 1–14, 2019. https://doi.org/10.1080/03772063.2019.1670103

[21] W. J. Okello, Q. Liu, F. A. Siddiqui, and C. Zhang, “A Survey of the Current State of Light-Weight Cryptography for the Internet of Things,” in 2017 International Conference on Computer, Information and Telecommunication Systems (CITS), 2017, pp. 292–296: IEEE.

[22] J. Yogi, U. S. Chauhan, A. Raj, M. Gupta, and S. S. Sudan, “Modeling Simulation and Performance Analysis of Lightweight Cryptography for IoT-Security,” in 2018 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE), 2018, pp. 1–5: IEEE. https://doi.org/10.1109/ICRAIE.2018.8710387

[23] A. Shamir, A. Biryukov, and L. P. Perrin, “Summary of an Open Discussion on IoT and Lightweight Cryptography,” in Proceedings of Early Symmetric Crypto Workshop, 2017, 2017: University of Luxembourg.

11 Author

Sinan Adnan Diwan, Asst. Prof. Dr. and Dean College of Science and Information Technology, Wasit University, Iraq. His Bachelor degree in Computer Science from Baghdad University College of Science, Iraq. His Master degree in Computer Science from Al-Mustansria University. Iraq. His Ph.D. degree in Information Technology from Limkokwing University of Creative Technology, Malaysia (sdiwan@uowasit.edu.iq).

Article submitted 2022-02-08. Resubmitted 2022-03-10. Final acceptance 2022-03-11. Final version published as submitted by the authors.