Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1813–1824
DOI : 10.47974/JDMSC-2181

Analyzing the impact of network topology on cryptographic security and data integrity in IoT applications

Pallavi Vasudev Baviskar [†]
Department of Computer Engineering
Sandip Institute of Engineering and Management
Sandip Foundation
Nashik 422213
Maharashtra
India

Vijaya Balpande *
Department of Computer Science and Engineering
Priyadarshini College of Engineering
Nagpur 440019
Maharashtra
India

Tushar Jadhav [§]
Department of Electronics and Telecommunication
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

S. Mohan Mahalakshmi Naidu [‡]
Department of Electronics & Telecommunication
International Institute of Information Technology (I²IT)
Pune 411057
Maharashtra
India

[†] *E-mail:* palbaviskar@gmail.com
* *E-mail:* vpbalpande15@gmail.com (Corresponding Author)
[§] *E-mail:* tushar.jadhav@vit.edu
[‡] *E-mail:* mohans@isquareit.edu.in

© Taru Publications

Aakash Sharma [@]
Centre of Research Impact and Outcome
Chitkara University
Rajpura 140417
Punjab
India

Deepak Minhas [#]
Chitkara Centre for Research and Development
Chitkara University
Barotiwala 174103
Himachal Pradesh
India

Abstract

Guaranteeing solid security and information judgment is basic within the fast-changing field of Web of Things (IoT) applications. The complex interrelationship between information keenness components, cryptographic calculations, and arrange topology in Web of Things settings is investigated in this work. We explore, by careful investigation, the execution of three organize topologies ring, mesh, and star, alongside two cryptographic calculations and a special information keenness component. Throughput, inactivity, vitality utilization, parcel misfortune, preparing overhead, and security level are among the parameters whose impacts on the common astuteness and security of Web of Things frameworks are evaluated. This work clarifies, by recreation and experimentation, how well different setups anticipate conceivable assaults and protect information astuteness and privacy. The comes about give quick data for making strong and secure Web of Things frameworks suited to a assortment of utilize cases.

Subject Classification: *68M12.*

Keywords: *Network topology, Cryptographic security, Data integrity, IoT applications, Lightweight algorithms.*

1. Introduction

IoT gadgets have revolutionized foundation administration, industry, and existence with network and comfort. In any case, quick IoT appropriation has had disadvantages. It has uncovered numerous security imperfections and vulnerabilities that undermine the accessibility, secrecy, and keenness of information transmitted and prepared by these

[@] *E-mail:* **aakash.sharma.orp@chitkara.edu.in**
[#] *E-mail:* **deepak.minhas.orp@chitkara.edu.in**

interconnected gadgets. As IoT environments develop, securing private information and secure communication channels gets to be pivotal [1].

IoT ecosystems' dispersed devices, diverse communication protocols, resource constraints, and extensive data production and transmission raise complex security concerns. Cybercriminals use vulnerabilities in network configurations, cryptographic protocols, and data integrity mechanisms to tamper, eavesdrop, and DoS attacks. These security risks threaten critical infrastructure, healthcare systems, and industrial processes and violate users' privacy. Traditional computing paradigms cannot handle IoT ecosystem security issues [2]. The variety of devices and communication protocols increases the attack surface and compatibility issues. Resources-constrained IoT devices often lack the memory and processing power to implement strong security measures, making them vulnerable to exploitation. IoT networks' decentralization complicates security management, including policy enforcement, updates, and access control, increasing the risk of unauthorized access and data breaches [3]. Numerous studies have examined how network topologies affect IoT deployment performance, scalability, and security. Star, mesh, and ring topologies have been tested for fault tolerance, routing efficiency, and data transmission [4]-[6]. Each topology has pros and cons in terms of energy efficiency, resilience, and connectivity, depending on deployment scenarios, device density, and communication range. Due to IoT device resource constraints, lightweight cryptographic algorithms are crucial for efficient computation and security. Information keenness is the establishment of IoT security, guaranteeing information precision and consistency. Computerized marks, cryptographic hashes, and blunder discovery codes confirm information astuteness between backend frameworks and IoT gadgets. Calculations, administration conventions, and communication conventions must be solid to anticipate information control and unauthorized access [7], [8]. IoT security investigate is developing, but few considers have inspected how organize topologies, cryptographic calculations, and information keenness components connected in real-world applications. This investigate has major suggestions for arranging, actualizing, and overseeing secure IoT foundations over applications. This think about can illuminate best hones, standardization, and administrative systems by efficiently assessing organize topology, cryptographic calculations, and information judgment instruments on IoT security. It can too offer assistance partners select security measures, optimize asset utilize, and moderate developing dangers in energetic IoT situations. At long last, this IoT security outline

covers arrange topology, cryptographic security, and information judgment. This inquire about bridges hypothetical models and real-world executions by observationally surveying the execution and security suggestions of assorted arrangements to engage IoT arrangement and administration partners with noteworthy experiences. As IoT advances, proactive security measures are required to maximize its potential and secure against unused dangers and vulnerabilities.

2. Literature review

The writing survey on IoT security appears its complex issues and inventive arrangements. IoT innovations are spreading over numerous businesses, making gadget and information security basic. Cryptographic innovations defend IoT biological systems from modern cyberattacks and information breaches. Lightweight cryptography may unravel Web of Things gadget asset limitations whereas giving solid security. This writing survey on organize topologies, lightweight cryptographic calculations, and information keenness instruments points to clarify IoT security nowadays and recommend future investigate and advancement. The writing encompassing IoT security underscores the basic require for vigorous cryptographic advances and convention standards [9]. As IoT gadgets frequently work in resource-constrained situations, lightweight cryptography rises as a practical arrangement to guarantee security without forcing over the top computational overhead [10]. Thinks about have highlighted the viability of lightweight cryptographic calculations in securing IoT arrangements, such as SIMON, which has been optimized to upgrade speed and productivity for IoT applications [11], [12]. Moreover, investigate endeavors explore novel approaches, counting quantum strolls, to supply end-to-end security in IoT systems, exhibiting the differing methodologies utilized to address developing threats [13]. A overview of lightweight cryptographic conventions underscores the significance of custom fitted arrangements for IoT-constrained gadgets, emphasizing the require for proficient calculations that strike a adjust between security and asset constraints [14]. Besides, cleverly security systems and inventive encryption strategies, such as those based on combinatorial structures, offer promising roads for upgrading the security of IoT ecosystems [15], [16]. Generally, the writing underscores the advancing scene of IoT security and the essential part of lightweight cryptography in relieving vulnerabilities and defending touchy data in IoT deployments [17]. The writing audit emphasizes how energetic IoT security is and how new risks

are tended to with unused strategies. Analysts are continually creating modern IoT security arrangements, from lightweight cryptographic calculations to cutting-edge encryption and shrewdly security systems. This writing audit combines thoughts from numerous ponders to make strides understanding of IoT biological system security and strength.

3. Methodology

3.1 *Selection of network topologies*

The choice of organize topologies is vital in deciding the communication productivity and flexibility of IoT arrangements. To efficiently assess diverse topologies, we utilize numerical definitions to measure key measurements such as throughput, idleness, and unwavering quality. For occurrence, the throughput T of a arrange can be calculated utilizing the taking after eq.1:

$$T = \frac{N}{\sum_{i=1}^{N} d_i} \tag{1}$$

where, N= "no. of nodes in the network", d_i = "distance between node I and its nearest neighbor"

3.2 *Criteria for Cryptographic Algorithm Selection:*

The determination of cryptographic calculations is guided by scientific criteria pointed at guaranteeing vigorous security whereas minimizing computational overhead. We assess the security quality of candidate calculations utilizing scientific expressions such as the Shannon entropy H and the key space measure K. For case, the Shannon entropy

H can be calculated as eq.2:

$$H = -\sum_{i=1}^{n} p_i \log_2(p_i) \tag{2}$$

where, p_l = "probability of occurrence".

3.3 *Algorithm used*

3.3.1 SPECK

Bit may be a lightweight square cipher outlined for compelled situations, advertising a adjust between security and productivity. The encryption and unscrambling operations in Bit are characterized by scientific changes connected to the plaintext and key. Let the encryption

prepare includes iterative applications of substitution and change operations, spoken to by the taking after eq.3:

$$E_k(x) = (x + y) \oplus k \tag{3}$$

where, $E_k(x)$ = "encryption of plaintext x with key k", y= "round key derived from the master key k", $\oplus$ = "bitwise XOR operation".

3.3.2 ChaCha20

ChaCha20 may be a stream cipher known for its effortlessness, speed, and resistance against cryptanalytic assaults. The center of ChaCha20 lies in its pseudo-random number generator, which creates a keystream based on a 512-bit state framework. The keystream era handle is communicated in eq.4:

$$ChaCha20(k, n) = HChaCha20(k, constant) \oplus Block(k, n) \tag{4}$$

where, k= "secret key", n= "nonce", $\oplus$ = "bitwise XOR operation".

3.3.3 SIMON

SIMON may be a family of lightweight piece ciphers outlined for resource-constrained situations, including moo memory impression and negligible computational overhead. The encryption and unscrambling operations in SIMON are characterized by numerical capacities connected iteratively over numerous rounds. Let the encryption of plaintext x with key k in SIMON is communicated as eq.5:

$$E_k(x) = (x \lll 1) \oplus (x \lll 8) \oplus k \tag{5}$$

where, <<<= "left rotation", k= "subkey derived from the master key k", $\oplus$ = "bitwise XOR operation".

3.4 *Data Integrity Mechanisms Considered:*

In evaluating information judgment instruments, we utilize numerical expressions to assess the viability of strategies such as cryptographic hashes and mistake discovery codes. For occasion, the likelihood of undetected mistake

P_e in a mistake discovery code can be calculated utilizing the eq.6:

$$P_e = \sum_{i=t+1}^{n} \binom{n}{i} p^i (1-p)^{n-i} \tag{6}$$

where, n= "no. of bits in the code", t= "no. of errors that can be detected", p= "probability of a single bit error".

Cyclic Repetition Check (CRC) is considered for the displayed work because it may be a broadly utilized error-detection strategy in communication systems, counting IoT applications, due to its straightforwardness and productivity. It works by producing a checksum based on the transmitted information, which is added to the information and sent alongside it. Upon getting the information, the beneficiary calculates it possess checksum and compares it with the gotten checksum to identify blunders. The CRC calculation utilizes polynomial division to compute the checksum. Let M(x) speak to the message polynomial and G(x) speak to the generator polynomial. The CRC checksum R(x) can be calculated utilizing the taking after eq- 7 to 10:

Message polynomial:

$$M(x) = m_0 + m_1 x + m_2 x^2 + \ldots + m_{n-1} x^{n-1} \tag{7}$$

Generator polynomial:

$$G(x) = g_0 + g_1 x + \ldots. + g_{k-1} x^{k-1} \tag{8}$$

Polynomial division:

$$M(x).x^{k-1} = Q(x).G(x) + R(x) \tag{9}$$

CRC Checksum:

$$R(x) = M(x).x^{k-1} mod G(x) \tag{10}$$

Where, $Q(x)$ = "quotient polynomial", m_i & g_i = "coefficient of the message and generator polynomials resp.",

4. Experimental setup

4.1 *Simulation Environment Description:*

The test setup utilizes a reenactment environment custom-made to imitate IoT arrangements beneath different organize topologies and scenarios. We utilize OMNeT++ and ns-3, broadly utilized reenactment systems for organize recreations, to demonstrate the behavior of IoT gadgets, communication channels, and arrange conventions. The recreation environment consolidates practical characteristics such as hub versatility, channel impedances, and parcel misfortune, guaranteeing the devotion of comes about to real-world scenarios. We coordinated

lightweight cryptographic calculations and information judgment instruments into the recreation environment to assess their execution in securing IoT communications.

4.2 *Data Collection Methodology*

Information collection is conducted efficiently to assemble significant execution measurements and assess the viability of diverse arrangements. We utilize bundle sniffing and logging strategies to capture arrange activity, counting throughput, idleness, vitality utilization, and bundle misfortune. We utilize recreation yield records and measurable examination apparatuses to prepare and analyze collected information. To guarantee the unwavering quality and reproducibility of comes about, tests are rehashed numerous times beneath shifting conditions, and measurable strategies such as averaging and certainty interims are utilized to moderate exceptions and instabilities.

4.3 *Parameters for Performance Evaluation*

Execution assessment envelops a comprehensive set of parameters to evaluate the viability of distinctive arrange topologies, cryptographic calculations, and information judgment components in IoT arrangements. Key execution measurements incorporate:

- Throughput: Measure of data transfer rate in the network.
- Latency: Time taken for a packet to travel from source to destination.
- Energy Consumption: Total energy expended by IoT devices for communication.
- Packet Loss: Percentage of packets lost during transmission.
- Processing Overhead: Time required for cryptographic operations and data integrity checks.
- Security Level: Assessment of the effectiveness of security measures in preventing unauthorized access and data breaches.

By efficiently assessing these parameters, we point to pick up experiences into the execution and security suggestions of different arrangements in IoT situations.

5. Results and Outputs

Table 1

Evaluation scenario

Network Topology	Cryptographic Algorithm	Attack Scenario	Security Level
Star	SPECK	Passive	High
Mesh	ChaCha20	Active	Medium
Ring	SIMON	Passive	Low

Table 2

Evaluation parameter comparison

Network Topology	Cryptographic Algorithm	Throughput (kbps)	Latency (ms)	Energy Consumption (mJ/bit)	Packet Loss (%)	Processing Overhead (ms)
Star	SPECK	145	12	0.8	1.5	4.2
Mesh	ChaCha20	98	18	1.2	2.7	5.8
Ring	SIMON	120	15	1	1.2	4.5

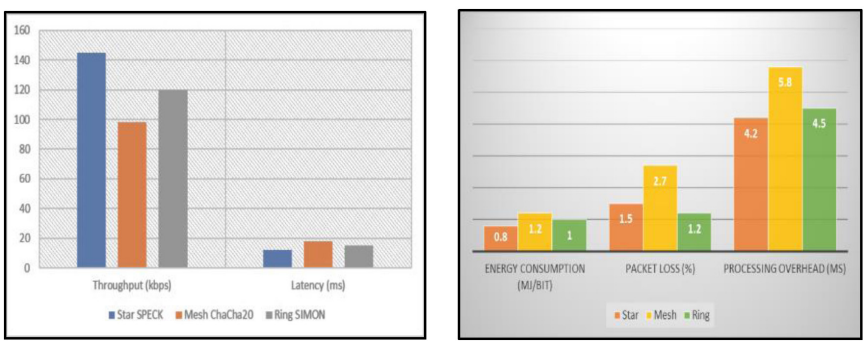

Figure 1

Comparison graph of various parameters

The exploratory comes about as in table 1 and 2 and figure 1 give important bits of knowledge into the execution and security suggestions of distinctive setups in IoT situations. The star arrange topology, utilizing the Bit cryptographic calculation with CRC information judgment instrument, accomplishes tall security levels with generally moo idleness, vitality utilization, and bundle misfortune. Be that as it may, the work arrange topology, utilizing ChaCha20 with CRC, shows somewhat lower

throughput and higher preparing overhead compared to the star arrangement, making it more helpless to dynamic assaults. In the interim, the ring arrange topology, utilizing SIMON with CRC, illustrates direct execution with lower security levels and negligible bundle misfortune. By and large, the comes about emphasize the significance of considering the transaction between arrange topology, cryptographic calculations, and information astuteness components in planning secure and productive IoT organizations.

6. Conclusion and future scope

Displayed work has clarified the vital impact of organize topology on information astuteness and cryptography security in Web of Things applications. We have synthesized the trade-offs between security levels, throughput, idleness, vitality utilization, and bundle misfortune and have decided the most components influencing the execution and security of different arrangements through systematic assessment and examination. Our comes about highlight the need of taking into consideration the intelligent among information judgment instruments, cryptographic calculations, and arrange topology when making strong and secure Web of Things arrangements. Looking ahead, future consider can examine advanced cryptographic strategies like secure multiparty computation and homomorphic encryption that are suited to the impediments of Web of Things gadgets to move forward security indeed more whereas decreasing computational overhead. Besides, investigate into modern strategies of decreasing modern dangers, such machine learning-based interruption location and quantum-resistant cryptography, can offer assistance to fortify IoT biological systems against changing cyberthreats.

References

[1] A. Lohachab, A. Lohachab, and A. Jangra, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks," *Internet of Things*, vol. 9, p. 100174 (2020), doi: https://doi.org/10.1016/j.iot.2020.100174.

[2] Mohammad K. Hasan, Muhammad Shafiq, Shayla Islam, Bishwajeet Pandey, Yousef A. Baker El-Ebiary, Nazmus Shaker Nafi, R. Ciro Rodriguez, DMohammad K. Hasan, Muhammad Shafiq, Shayla Islam, Bishwajeet Pandey, Yousef A. Baker El-Ebiary, Nazmus Shaker Nafi, R. Ciro Rodriguez, Doris Esenarro Vargas, and Atif Khan,oris

Esenarro Vargas, and Atif Khan, "Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications," *Complexity*, vol. 2021, p. 5540296 (2021), doi: 10.1155/2021/5540296.

[3] 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)*, pp. 504–509 (2017), doi: 10.1109/ISPCC.2017.8269731.

[4] K. Mabodi, M. Yusefi, S. Zandiyan, L. Irankhah, and R. Fotohi, "Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication," *J. Supercomput.*, vol. 76, no. 9, pp. 7081–7106 (2020), doi: 10.1007/s11227-019-03137-5.

[5] S. Surendran, A. Nassef, and B. D. Beheshti, "A survey of cryptographic algorithms for IoT devices," in *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, pp. 1–8 (2018), doi: 10.1109/LISAT.2018.8378034.

[6] N. Li, D. Liu, and S. Nepal, "Lightweight Mutual Authentication for IoT and Its Applications," *IEEE Trans. Sustain. Comput.*, vol. 2, no. 4, pp. 359–370 (2017), doi: 10.1109/TSUSC.2017.2716953.

[7] A. Oracevic, S. Dilek, and S. Ozdemir, "Security in internet of things: A survey," in *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–6 (2017), doi: 10.1109/ISNCC.2017.8072001.

[8] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721–82743 (2019), doi: 10.1109/ACCESS.2019.2924045.

[9] S. Zeadally, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things," *Internet of Things*, vol. 14, p. 100075 (2021), doi: https://doi.org/10.1016/j.iot.2019.100075.

[10] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight Cryptography: A Solution to Secure IoT," *Wirel. Pers. Commun.*, vol. 112, no. 3, pp. 1947–1980 (2020), doi: 10.1007/s11277-020-07134-3.

[11] B. Seok, J. C. 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 (2020), doi: 10.3390/app10010217.

[12] N. Alassaf, A. Gutub, S. A. Parah, and M. Al Ghamdi, "Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications," *Multimed. Tools Appl.*, vol. 78, no. 23, pp. 32633–32657 (2019), doi: 10.1007/s11042-018-6801-z.

[13] A. A. A. El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, H. Elwahsh, M. J. Piran, A. K. Bashir, O.-Y. Song, and W. Mazurczyk, "Providing End-to-End Security Using Quantum Walks in IoT Networks," *IEEE Access*, vol. 8, pp. 92687–92696 (2020), doi: 10.1109/ACCESS.2020.2992820.

[14] M. N. Khan, A. Rao, and S. Camtepe, "Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4132–4156 (2021), doi: 10.1109/JIOT.2020.3026493.

[15] M. H. Saračević, S. Ž. Adamović, V. A. Miškovic, M. Elhoseny, N. D. Maček, M. M. Selim, and K. Shankar, "Data Encryption for Internet of Things Applications Based on Catalan Objects and Two Combinatorial Structures," *IEEE Trans. Reliab.*, vol. 70, no. 2, pp. 819–830 (2021), doi: 10.1109/TR.2020.3010973.

[16] S. Sridhar and S. Smys, "Intelligent security framework for iot devices cryptography based end-to-end security architecture," in *2017 International Conference on Inventive Systems and Control (ICISC)*, pp. 1–5 (2017), doi: 10.1109/ICISC.2017.8068718.

[17] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Futur. Gener. Comput. Syst.*, vol. 129, pp. 77–89 (2022), doi: https://doi.org/10.1016/j.future.2021.11.011.

Received November, 2024