Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
May 2024 5(5), 342–351

IMPROVING SECURITY OF IOT DEVICE COMMUNICATION USING MODIFIED HASHING SOLUTION

B Bamleshwar Rao[1], Dr. Akhilesh A. Waoo[1]

[1] AKS University, SATNA, MP, India

ABSTRACT

Advancements in technology have led to the invention of outfits, and the number of devices is increasing every day. Diligence is introducing new devices day by day and prognosticating that 50 billion devices will be connected by 2022. These devices are stationed through the Internet, called the Internet of Things (IoT). The operation of IoT devices is weather prediction, covering surgery in hospitals, identification of creatures using biochips, furnishing shadowing connectivity in motorcars, smart home appliances, etc. IoT devices have limitations related to security at both the software and hardware ends. In the IoT paradigm, Internet-connected embedded devices manipulate sensitive user-related data and require acceptable security results.

The security results designed for network-enabled embedded devices must address issues like vacuity and usability, taking into consideration the low computational capabilities and low consumption conditions of IoT appliances. Authentication is the process of vindicating a reality's identity. Best security practices state that authentication protocol should involve at least two different types of credentials. Authentication in IoT is a bit challenging because the realities involved in the IoT terrain cannot afford to include cryptographic savages which have high computational complexity as in the traditional internet. The most recent secure hash algorithm fashion formalized by the NIST is SHA-3. SHA-3 is fully appropriate to ensure authentication for a sender and receiver transaction. The presented paper includes a deep literature review on IoT security issues and proposes a new modified hash algorithm, which is more efficient in device communication security.

Keywords: IoT security, authentication, device security, SHA, Token based authentication, Device communication, Modified hash

Corresponding Author

Akhilesh A. Waoo,
akhileshwaoo@gmail.com

DOI
10.29121/shodhkosh.v5.i5.2024.1885

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

1. INTRODUCTION

The so-called "Internet of Things" mainly refers to the information exchange between objects or devices through the Internet. It is an innovative technology grounded on advanced network information technologies such as computer technology and Internet technology and is also one of the main directions for the development and operation of network information technology [60]. The emergence and operation of the Internet of Things technology will greatly promote the enhancement of the degree of Informatization in related fields. In addition, it also has an important impact on the construction and operation of smart cities, smart hospitals the upgrading and transformation of industrial production, and people's daily lives. It also provides new ways and specialized support for working numerous backups that circumscribe social and profitable development.

The Internet of Things system structure, mainly includes the control layer, perception layer, processing layer, and transmission layer. Among them, the perception layer is mainly responsible for the collection and processing of data, the

application layer is responsible for the consummation of the Internet of Things business, and the network layer substantially relies on various network forms to complete data interaction [50]. IoT architecture is shown in Fig 1.

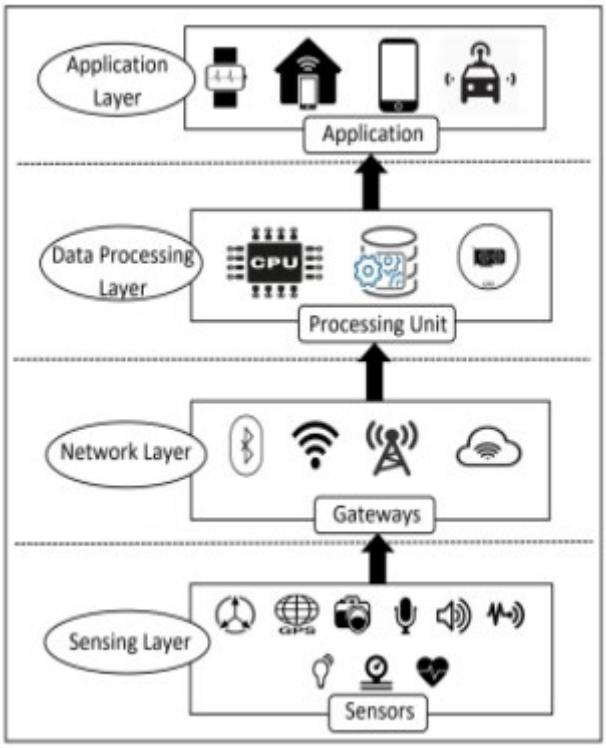

Figure 1: IoT architecture [58].

The infiltration of viruses and Trojan horses into computer networks seriously affects the security of the network terrain. Hackers' attacks on IoT vulnerabilities can pose serious trouble to the security of IoT and the security and privacy of IoT data and information [51]. Thus, to ensure information security in the Internet of Things, it is necessary to dissect various security risks and frequently use advanced information and information security technology to improve the ability of the Internet of Things to prevent unauthorized access. Attackers often use limited tools because they are neither safe nor unsafe. In the future, many cases will be reported of attackers using bots to control restricted objects and use them to launch DDoS attacks. In other words, the IoT environment requires heavy security measures. They need a strong authentication process to ensure networks and devices are secure. Authentication is the process of vindicating the identity of a reality. New "smart" services and smart devices, smart homes, smart watches, smart TVs, etc. Due to the emergence of IoT devices, they are rapidly becoming widespread and widespread in many areas. Additionally, many of these smart services require users to deliberately disclose some personal information (sometimes private) to receive enhanced and personalized services. Security and privacy must be a priority in the development of IoT technology and services. Unfortunately, this is not the case for many IoT products with insufficient, missing, or poorly designed security mechanisms. In the past few years, recording video in a private environment has become increasingly important over time, as personal space, health, etc. There are growing concerns about the risks associated with using essential IoT devices in services that may access sensitive or critical information like monitoring, home management, business, and lighting [21], [43]. Some security attacks on commercial IoT devices have also appeared in popular media, helping to raise public security awareness about threats to the IoT world.

To make commercial IoT devices more resilient to cyber-attacks, security should be taken into account right from the design stage of new products [36]. However, the wide heterogeneity of IoT devices hinders the development of well-established security-by-design methods for the IoT [26], [35]. The severe limits in energy, communication, calculation, and storehouse capabilities of many IoT devices further complicate the challenge. Such limits indeed prevent the possibility of adopting standard security mechanisms used in more traditional Internet-connected devices [53], and call for new results that, however, aren't yet formalized.

Many IoT device manufacturers come from the market of low-cost sensors and actuators (e.g., home automation, light control, video surveillance, and so on). Such devices were originally designed to work in isolated systems, for which the security threats are much more limited. Consequently, many manufacturers do not possess solid expertise in cybersecurity and may be unaware of the security risks associated with connecting their devices to a global network. A lack of ignorance along with the hectic approach to the design of new products and the necessity to compress costs and time-to-market have led to the commercialization of IoT products where security is neglected [9]. A survey from the McKinsey Global Institute estimates investments in the Internet of Things (IoT) to be over $11 trillion by 2025 [7]. Indeed, the use of IoT devices in corporate and industrial environments is currently skyrocketing. In most cases, these IoT devices, which have limited computing resources and diverse communication capabilities [20], share access to sensitive information with other networking devices (e.g., servers and gateways) present in corporate networks and critical systems [31], [32], [33], [54], [55]. In these settings, hackers can gain unauthorized access to the networks and impersonate legitimate IoT devices via spoofing attacks. For instance, using a spoofed device, the attackers can steal sensitive information, inject illegitimate data into the system, or implement targeted attacks over other devices, while mimicking legitimate device operations [1],[6],[25],[28]. The high diversity of devices and communication protocols (e.g., Internet Protocol (IP), ZigBee, Zwave) present in IoT devices makes defending against spoofing attacks extremely difficult. Passive device-class fingerprinting techniques can be used to identify the type of resource-limited devices present in the network and detect unauthorized devices. Although there is a substantial amount of research in fingerprinting techniques for IP- and Bluetooth-enabled IoT devices, there exist no solutions to identify IoT devices that communicate via ZigBee or Z-Wave, which are very popular in current smart office and home settings [30], [2]. Since different communication protocols typically implement a unique protocol stack and network architecture, IP- and Bluetooth-based identification solutions would not effectively fingerprint ZigBee- or Z-Wave-enabled devices.

IoT system is composed of three components such as a sensing unit having a large number of sensors, actuators, and mobile terminals to detect the physical environments [11]. This fragile and simple structure of IoT makes it more vulnerable to the threats related to the security of IoT. Besides, IoT devices suffer from other various security issues and challenges. These security issues and challenges were addressed by various approaches by different authors. However, we systematically reviewed the analysis of IoT-based devices by using the concepts of network security of IoT devices while in communication. To address the security issues after analyzing all the major threats, we integrated the Security IoT system.

The communication among the IoT devices is machine-to-machine (M2M) without the involvement of humans. In hardware-based solutions where only sensors, actuators, and processors are used security procedures and policies within the smartphone, laptop, palmtop, etc. are more robust and efficient. These devices can be connected with IoT devices to secure them Smartphones can be used as controller home automation systems and IoT devices can be authenticated by using a smart smartphone as a QR-code authenticator [52], [37]. Mobile devices can also be used as IoT middleware that is designed specifically for low-powered resource-constrained to process data easily from sensors [10]. Similarly, mobile computing through various applications, services, or other infrastructure could affect the IoT devices' security. In this regard, mobile applications and IoT will be the most disruptive class of technologies in the next 10 years [16]. Mobile applications in the context of IoT management can play a vital role. The IoT device's vulnerability could be easily compromised, the IoT mobile apps can be reckoned as helpful to disintegrate this vulnerability but the development of such apps could be a challenging task as such apps are not like mobile applications because they contain web, mobile, and networking components. The IoT has many applications and thus it is needed to collect personal information, IoT is experiencing some more serious privacy security risks [48]. Similarly, the current IoT devices available in the market with lousy security, leading to vulnerabilities that will ‘‘affect flesh and blood’’ [41]. We need some solutions to address these security and privacy risks. This paper presents a new method of hashing for providing security to IoT device communication.

2. RELATED WORKS

IoT devices are pervasive and ubiquitous as per prediction the number of IoT devices to be 50 billion by 2020 [24]. With the rise of this mammoth elevation in number, security has become a burning issue and has grabbed a great deal of attention in the last few years. Security is important from device to device as it deals with the end-to-end communication

between individual devices [13]. Strong security is a dire need of IoT due to the rapid rise in IoT devices and cyber-attacks [40]. In this regard, various reviews have suggested mechanisms to cope with the security problems and challenges of IoT. Security analysis of IoT by using a systematic approach has been performed by different authors with different aspects but the main focus of this research work is to analyze the security of IoT by using the concepts of mobile computing. The security analysis of IoT by using mobile computing is a novel approach and it is the first attempt to analyze the security of IoT devices in light of mobile computing. The types of security threats for IoT are shown below[59]:

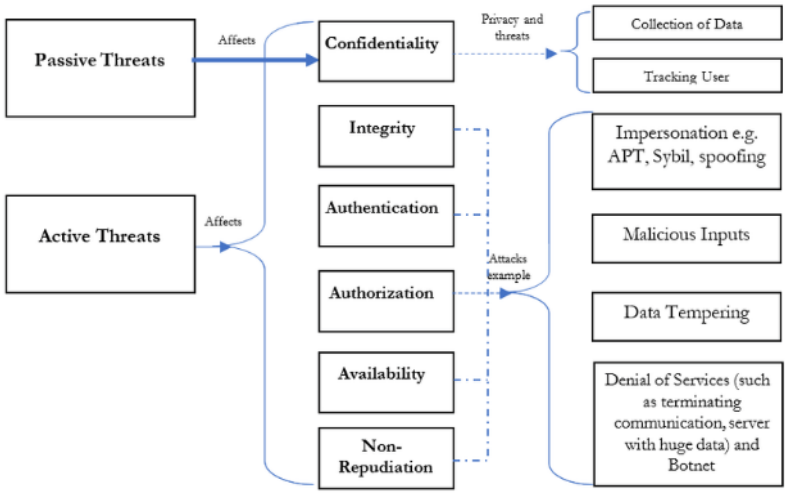

Figure 2: Security threats in IoT[59]

Systematic approaches for security analysis of IoT are bandied like Mohammadi et al. [47] performed SLR and presented trust-based IoT recommendation ways. Bhandari and Gupta [18] performed a systematic review based on fault analysis of IoT. Fazal et al. [29] analyzed the security of IoT through a systematic approach and they focused on highlighting and classifying the security challenges in three different aspects such that hardware, network, and cloud server. Aly et al. [34] systematically analyzed the security issues of IoT based on different layers. Macedo et al. [14] conducted SLR to analyze the security based on four security aspects such as trust, access control, data protection, and authentication. Martinez et al. [27] highlighted threats, attacks, challenges, and countermeasures related to the security of IoT. Similarly, Witti and Konstantas [38] evaluated the existing security and privacy issues through a systematic mapping study. Sultan et al. [4] analyzed the security issues and provided a solution by using blockchain technology.

With the popularity of computer hardware devices, the network technology based on this hardware has influenced and deeply affected all aspects of people's work and lives. The development of network technology further promotes the development of Internet of Things technology grounded on it. The development of the Internet of Things has greatly bettered effectiveness and convenience, but at the same time, there are numerous security pitfalls. Because of the failings of these mechanisms espoused by the current Internet of Things security convergence algorithm, this paper [17] proposes a network security discovery algorithm grounded on association rule mining. This algorithm avoids the frequency of IoT bumps grounded on the timestamp medium, improves the read-write conflict of IoT bumps, and improves the confluence rate of network security. It can meet the online security discovery and analysis of large-scale networks, effectively break the blights of current network security discovery algorithms, and ameliorate the security of data transmission and storehouse in Internet of Effects operations.

The current literature about the security analysis of IoT devices is categorized as depicted in Table 1.

Table 1: Major research in the field

Ref./Year	Techniques Used	Application
[42]/2022	Rivest Cipher (RC6) and SHA-256.	Efficient access control mechanism for Internet of Medical Things-based health care system.

[57]/2022	Improved elliptic curve digital signature algorithm	Industrial IoT Security.
[56]/2022	PKI digital certificate.	Certificate Authority (CA) for cloud IoT systems
[3]/2021	Grayscale using steganographic coding.	Secure implementation of data transmission in the IoT system
[23]/2020	SHA-3 Algorithm.	SHA-3 Co-Processor in Field-Programmable Gate Array.
[12]/2020	Novel graphical security model to capture malware spread in IoT.	Graphical security mode for Mirai.
[44]/2019	AES Algorithm	Car Tracking System Using IoT
[48]/2019	Elliptic curve cryptography	Hardware-accelerated DTLS for IoT Security.

3. PROPOSED SYSTEM

The proposed system architecture is shown below:

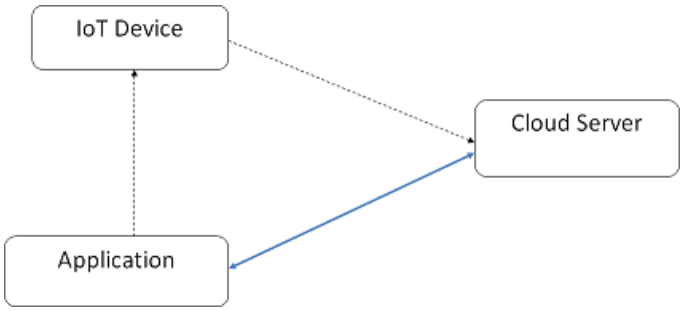

Figure 2: Proposed architecture.

In the proposed system, there will be three modules, IoT device, Cloud Server, and application. The IoT device will be wearable. This device will be attached to various sensors and will send the data to the Cloud Server for further analysis. Application is the system for accessing data.

The diagram below shows the flow of the proposed system:

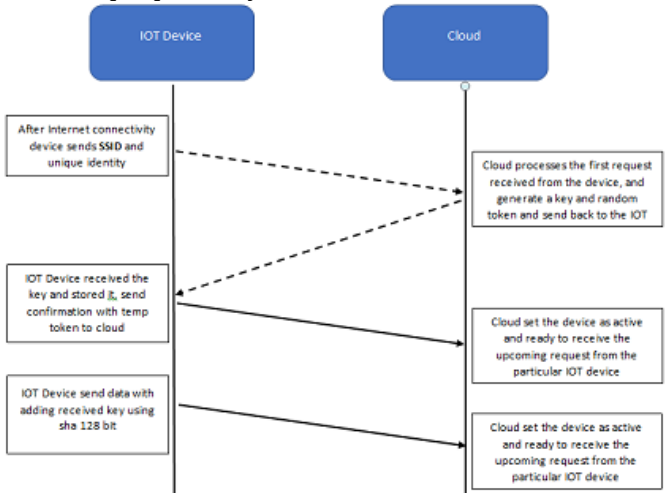

Figure 3: Proposed flow.

The algorithm for secure data communication between IoT devices and the cloud is as follows:

1. Start IoT Device or Reset.

2. Open the Android app and scan for IoT devices.
3. Connect the device using a web page with a specific IP address.
4. Set router SSID and password to IoT device of working internet.
5. After fixing it IoT device is ready to connect with the cloud system.
6. IoT devices send payload to our cloud system and the cloud recognizes the IoT device.
7. Cloud system checks the IoT device entry in the database. Whether it is available or not if available then responds unique payload to an IoT device.
8. IoT device receives payload data extracts it and saves it to memory.
9. After completion of handshaking. A secure connection has been established.
10. IoT device sends data to the cloud: first, get the value from the sensor then add a modified hash with the stored token received from the cloud and send it to the cloud.
11. Cloud receives hash then decodes with the same key and reads data.

4. RESULTS

The proposed system has designed a token-based authentication system that identifies users and devices. The research had also designed and modified a secure Hashing Solution. The system has device tokens shown in the figure below:

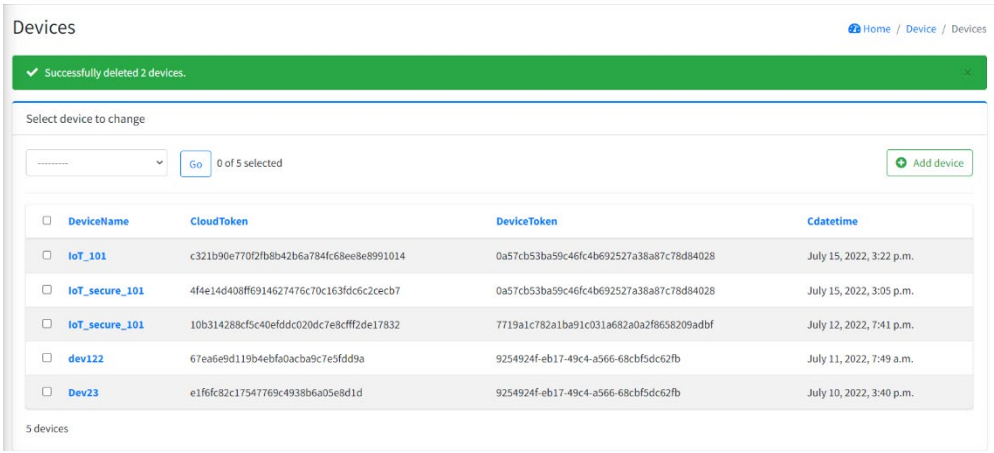

Figure 4: Device token.

A snapshot of data received from the IoT device is shown below:

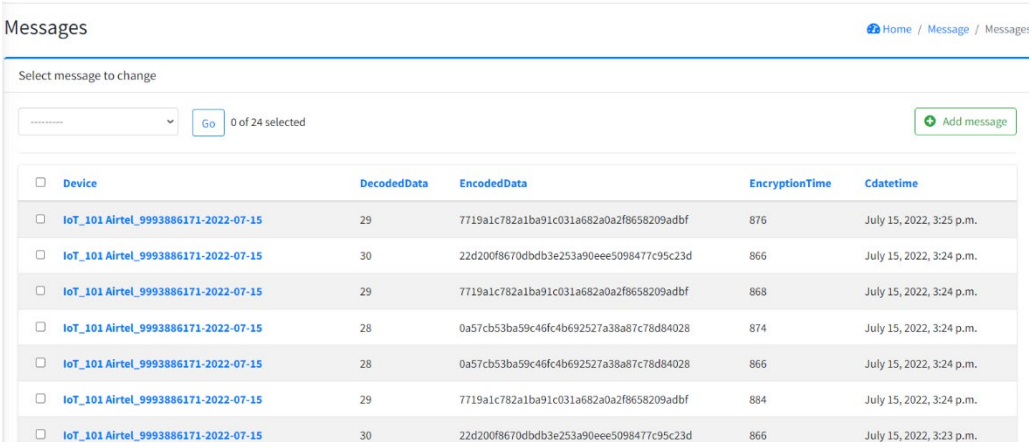

Figure 5: Data received from IoT device.

The proposed system has modified the existing SHA method. The result below shows a comparison of SHA and modified SHA used in the proposed system:

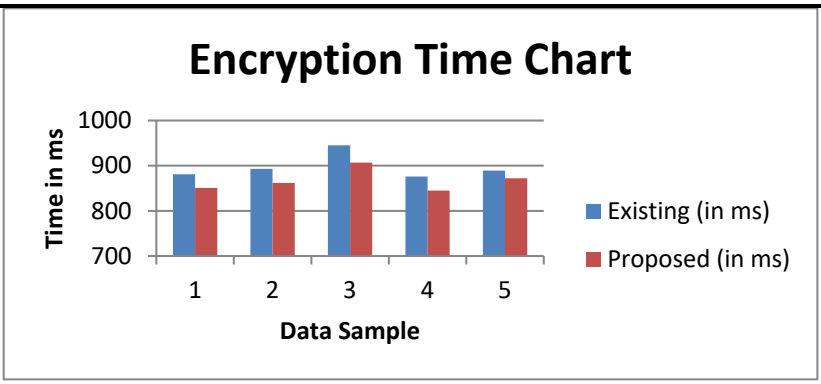

Figure 6: Comparison between existing and modified hash methods for encryption time.

5. Conclusions

Improving security and reducing risks in information systems depend heavily on analyzing threats, risks, and vulnerabilities to develop the appropriate countermeasures to mitigate their exploitations. A more challenging problem is to design an authentication scheme that can identify users for devices that don't maintain permanent contact with users. The proposed system has been found more secure and less complex. We have analyzed the proposed research with some existing research in a tabular form shown below:

Table 2: Comparative with existing research

Method	Implementation	Complexity	Overhead	User anonymity	Prone to attack
[39]	Easier	High	More	Yes	Yes
[15]	Complex	High	More	Yes	Yes
[45]	Complex	High	More	Yes	Yes
Proposed	Easier	Low	Less	No	More enhanced

CONFLICT OF INTERESTS

None

ACKNOWLEDGMENTS

None

REFERENCES

"Method of Resource-limited Device and Device Class Identification Using System and Function Call Tracing Techniques, Performance, and Statistical Analysis," Patent 10 242 193.

K. Sikder, L. Babun, H. Aksu, and A. S. Uluagac, "Aegis: A Context-Aware Security Framework for Smart Home Systems," ser. ACSAC 2019.

Kabulov, I. Saymanov, I. Yarashov and F. Muxammadiev, "Algorithmic method of security of the Internet of Things based on steganographic coding," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-5, doi: 10.1109/IEMTRONICS52119.2021.9422588.

Sultan, M. S. Arshad Malik, and A. Mushtaq, "Internet of Things security issues and their solutions with blockchain technology characteristics: A systematic literature review," Amer. J. Comput. Sci. Inf. Technol., vol. 6, no. 3, p. 27, 2018.

Wang, "Internet of Things Computer Network Security and Remote Control Technology Application," 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), 2020, pp. 1814-1817, doi: 10.1109/ICMCCE51767.2020.00398.

Babun, Leonardo, Aksu, Hidayet, Uluagac, S. A., "Detection of Counterfeit and Compromised Devices Using System and Function Call Tracing Techniques," Patent 10 027 697.

By 2025, Internet of Things applications could have $11 trillion impact, https://www.mckinsey.com/mgi/overview/in-the-news/ by-2025-internet-of-things-applications-could-have-11-trillion-impact, 2019.

Kaygusuz, L. Babun, H. Aksu, and A. S. Uluagac, “Detection of Compromised Smart Grid Devices with Machine Learning and Convolution Techniques,” in 2018 ICC.

Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and other botnets,” Computer, vol. 50, no. 7, pp. 80–84, Jul. 2017.

Perera, P. P. Jayaraman, A. Zaslavsky, D. Georgakopoulos, and P. Christen, “MOSDEN: An Internet of Things middleware for resource-constrained mobile devices,'' in Proc. 47th Hawaii Int. Conf. Syst. Sci., Jan. 2014, pp. 1053_1062.

C.-T. Li, T.-Y.Wu, C.-L. Chen, C.-C. Lee, and C.-M. Chen, “An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system,'' Sensors, vol. 17, no. 7, p. 1482, Jun. 2017.

S. Kim, K. O. Chee, and M. Ge, "A Novel Graphical Security Model for Evolving Cyber Attacks in Internet of Things," 2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S), 2020, pp. 57-58, doi: 10.1109/DSN-S50200.2020.00031.

Buenrostro, D. Cyrus, T. Le, and V. Emamian, “Security of IoT devices,'' J. Cyber Secur. Technol., vol. 2, no. 1, pp. 1_13, 2018.

E. L. C. Macedo, E. A. R. de Oliveira, F. H. Silva, R. R. Mello, F. M. G. Franca, F. C. Delicato, J. F. de Rezende, and L. F. M. de Moraes, “On the security aspects of Internet of Things: A systematic literature review,'' J. Commun. Netw. vol. 21, no. 5, pp. 444_457, Oct. 2019.

E.H. Teguig & Y. Touati, “Security in Wireless Sensor Network and IoT: An Elliptic Curves Cryptosystem based Approach”, IEEE, 2018

Alshahwan, “Adaptive security framework in Internet of Things (IoT) for providing mobile cloud computing,'' in Mobile Computing Technology and Applications. London, U.K.: IntechOpen, 2018.

Guo, "Research on Security Convergence Algorithm of Internet of Things Based on Association Rules Mining," 2021 International Conference on Networking, Communications and Information Technology (NetCIT), 2021, pp. 121-124, doi: 10.1109/NetCIT54147.2021.00031.

G. P. Bhandari and R. Gupta, “A systematic literature review in fault analysis for IoT,'' Int. J. Web Sci., vol. 3, no. 2, pp. 130_147, 2019.

Guo Jinhua, Ming Xiaobo. “Internet of Things Computer Network Security and Remote Control Technology”, [J]. Contemporary Educational Practice and Teaching Research, 2016(3):264.

Aksu, L. Babun, M. Conti, G. Tolomei, and A. S. Uluagac, “Advertising in the IoT Era: Vision and Challenges,” IEEE Communications Magazine, 2018.

H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. F. Cranor, and Y. Agarwal, “Your location has been shared 5,398 times!: A field study on mobile app privacy nudging,” in Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2015, pp. 787–796.

Han Junfeng, “Analysis of Internet of Things Computer Network Security and Remote Control Technology” [J]. China New Communications, 2019, 21(21): 160.

L. R. Azevedo, A. S. Nery and A. d. C. Sena, "A SHA-3 Co-Processor for IoT Applications," 2020 Workshop on Communication Networks and Power Systems (WCNPS), 2020, pp. 1-5, doi: 10.1109/WCNPS50723.2020.9263759.

Ahamed and A. V. Rajan, ``Internet of Things (IoT): Application systems and security vulnerabilities,'' in Proc. 5th Int. Conf. Electron. Devices, Syst. Appl. (ICEDSA), Dec. 2016, pp. 1_5.

J. D. Fuller and B. W. Ramsey, “Rogue Z-Wave Controllers: A Persistent Attack Channel,” in 2015 LCN Workshops, 2015.

J. Granjal, E. Monteiro, and J. S. Silva, “Security for the Internet of Things: A survey of existing protocols and open research issues,” IEEE Communications Surveys Tutorials, vol. 17, no. 3, pp. 1294–1312, Jan. 2015.

J. Martinez, J. Mejia, and M. Munoz, “Security analysis of the Internet of Things: A systematic literature review,'' in Proc. Int. Conf. Softw. Process Improvement (CIMPS), Oct. 2016, pp. 1_6.

Denney, E. Erdin, L. Babun, M. Vai, and S. Uluagac, “USB-Watch: A Dynamic Hardware-Assisted USB Threat Detection Framework,” in Security and Privacy in Communication Networks, 2019.

K. Fazal, H. Shehzad, A. Tasneem, A. Dawood, and Z. Ahmed, “A systematic literature review on the security challenges of Internet of Things and their classification,'' Int. J. Technol. Res., vol. 5, no. 2, pp. 40_48, 2017.

Babun, A. K. Sikder, A. Acar, and A. S. Uluagac, “IoTDots: A Digital Forensics Framework for Smart Environments,” 2018. [Online]. Available: https://arxiv.org/pdf/1809.00745.pdf.

L. Babun, H. Aksu, and A. S. Uluagac, “A System-level Behavioral Detection Framework for Compromised CPS Devices: Smart-Grid Case,” IEEE Transactions on Cyber-Physical Systems, October 2019.

L. Babun, H. Aksu, and A. S. Uluagac, “Identifying Counterfeit Smart Grid Devices: A Lightweight System Level Framework,” in 2017 ICC, May 2017.
L. Babun, Z. B. Celik, P. McDaniel, and A. S. Uluagac, “Real-time Analysis of Privacy-(un)aware IoT Applications,” 2019. [Online]. Available: https://arxiv.org/pdf/1911.10461.pdf.
Aly, F. Khomh, M. Haoues, A. Quintero, and S. Yacout, “Enforcing security in Internet of Things frameworks: A systematic literature review,'' Internet Things, vol. 6, Jun. 2019, Art. no. 100050.
M. M. Hossain, M. Fotouhi, and R. Hasan, “Towards an analysis of security issues, challenges, and open problems in the Internet of Things,” in Proceedings of IEEE World Congress on Services, Jun. 2015, pp. 21–28.
M. R. Warner, “Internet of Things Cybersecurity Improvement Act of 2017,” S. 1691, 115th US Congress, Sep. 2017.
M. Togan, B.-C. Chifor, I. Florea, and G. Gugulea, “A smart-phone based privacy-preserving security framework for IoT devices,'' in Proc. 9th Int. Conf. Electron., Comput. Artif. Intell. (ECAI), Jun. 2017, pp. 1_7.
M. Witti and D. Konstantas, “IOT and security-privacy concerns: A systematic mapping study,'' Int. J. Netw. Secur. Appl., vol. 10, no. 6, pp. 25_33, Nov. 2018.
Ö. Yerlikaya and G. Dalkılıç, "Authentication and Authorization Mechanism on Message Queue Telemetry Transport Protocol," 2018 3rd International Conference on Computer Science and Engineering (UBMK), Sarajevo, Bosnia and Herzegovina, 2018, pp. 145-150, doi: 10.1109/UBMK.2018.8566599.
R. Gurunath, M. Agarwal, A. Nandi, and D. Samanta, “An overview: Security issue in IoT network,'' in Proc. 2nd Int. Conf. IoT Social, Mobile, Anal. Cloud (I-SMAC), Aug. 2018, pp. 104_107.
R. Roman-Castro, J. Lopez, and S. Gritzalis, “Evolution and trends in IoT security,'' Computer, vol. 51, no. 7, pp. 16_25, 2018.
S. M. Nagarajan, G. G. Deverajan, U. Kumaran, M. Thirunavukkarasan, M. D. Alshehri and S. Alkhalaf, "Secure Data Transmission in Internet of Medical Things Using RES-256 Algorithm," in IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 8876-8884, Dec. 2022, doi: 10.1109/TII.2021.3126119.
S. Misbahuddin, J. A. Zubairi, A. Saggaf, J. Basuni, S. A-Wadany, and A. Al-Sofi, “IoT based dynamic road traffic management for smart cities,” in Proceedings of the 12th International Conference on High capacity Optical Networks and Enabling/Emerging Technologies, Dec. 2015, pp. 1–5.
T. N. Dang and H. M. Vo, "Advanced AES Algorithm Using Dynamic Key in the Internet of Things System," 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS), 2019, pp. 682-686, doi: 10.1109/CCOMS.2019.8821647.
Trusit Shah and S. Venkatesan, “Authentication of IoT Device and IoT Server Using Secure Vaults”, IEEE, 2018
U. Banerjee, A. Wright, C. Juvekar, M. Waller, Arvind and A. P. Chandrakasan, "An Energy-Efficient Reconfigurable DTLS Cryptographic Engine for Securing Internet-of-Things Applications," in IEEE Journal of Solid-State Circuits, vol. 54, no. 8, pp. 2339-2352, Aug. 2019, doi 10.1109/JSSC.2019.2915203.
V. Mohammadi, A. M. Rahmani, A. M. Darwesh, and A. Saha, “Trust-based recommendation systems in Internet of Things: A systematic literature review,'' Hum.-Centric Comput. Inf. Sci., vol. 9, no. 1, p. 21, Dec. 2019.
W. Xi and L. Ling, “Research on IoT privacy security risks,'' in Proc. Int. Conf. Ind. Informat.-Comput. Technol., Intell. Technol., Ind. Inf. Integr. (ICIICII), Dec. 2016, pp. 259_262.
Wang Shixin. A preliminary study on computer network security and remote control technology of the Internet of Things [J]. Electronic Technology and Software Engineering, 2018(12):233.
Wang Zhiqiang. Preliminary study on computer network security and remote control technology of Internet of Things [J]. Electronic Testing, 2020(13): 96-97.
Wen Jinhui. Discussion on Internet of Things Computer Network Security and Its Remote Control Technology [J]. Electronic Testing, 2020(10): 69-70.
X. Su, Z.Wang, X. Liu, C. Choi, and D. Choi, “Study to improve security for IoT smart device controller: Drawbacks and countermeasures, Secure Communication Network, vol. 2018, pp. 1_14, May 2018.
Y. B. Saied, “Collaborative security for the Internet of Things,” Ph.D. dissertation, Institute National des Telecommunications, Jun. 2013.
Z. B. Celik, L. Babun, A. K. Sikder, H. Aksu, G. Tan, P. McDaniel, and A. S. Uluagac, “Sensitive Information Tracking in Commodity IoT,” in 27th USENIX.
Z. B. Celik, P. McDaniel, G. Tan, L. Babun, and A. S. Uluagac, “Verifying Internet of Things Safety and Security in Physical Spaces,” IEEE Security Privacy.

Z. Siddiqui, J. Gao and M. K. Khan, "An Improved Lightweight PUF-PKI Digital Certificate Authentication Scheme for the Internet of Things," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2022.3168726.

Z. Wang, "Research on edge data Processing security technology in Industrial Internet," 2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA), 2022, pp. 1102-1108, doi: 10.1109/CVIDLICCEA56201.2022.9824602.

Mohammed Ghazi Sami, Teba & Zeebaree, Subhi & Ahmed, Sarkar. "A Comprehensive Review of Hashing Algorithm Optimization for IoT Devices". International Journal of Intelligent Systems and Applications in Engineering. IJISAE, 2023, 11. 205–231.

Abbas, Ghulam & Mehmood, Amjad & Carsten, Maple & Epiphaniou, Gregory & Lloret, Jaime. "Safety, Security and Privacy in Machine Learning Based Internet of Things.",2022 Journal of Sensor and Actuator Networks. 11. 38. 10.3390/jsan11030038.

Jay Kumar Jain, & Waoo, A. A. . (2023). An Artificial Neural Network Technique for Prediction of Cyber-Attack using Intrusion Detection System. Journal of Artificial Intelligence, Machine Learning and Neural Network (JAIMLNN) ISSN: 2799-1172, 3(02), 33–42. https://doi.org/10.55529/jaimlnn.32.33.42