IMPLEMENTING TOKEN-BASED AUTHENTICATION AND MODIFIED HASHING FOR IOT SECURITY

B Bamleshwar Rao [1], Akhilesh A Waoo [2]

[1] AKS University, SATNA, MP, India

Corresponding Author

Akhilesh A Waoo,
akhileshwaoo@gmail.com

DOI
10.29121/shodhkosh.v5.i1.2024.1880

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

ABSTRACT

The Internet of Things system structure mainly includes a 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 realization of the Internet of Things business, and the network layer mainly relies on various network forms to complete data interaction [1]. Specific to the actual application of the Internet of Things technology, its application system generally includes a central server, a monitoring center, a wireless transmission network, a remote client, a server, various communication modules, and corresponding sensing devices. Its specific technical structure.

Keywords: IoT, Gateway, Control Security Technology

1. INTRODUCTION

"Internet of Things" mainly refers to the information exchange between objects or devices through the Internet. It is an innovative technology based on advanced network information technologies such as computer technology and Internet technology and is also one of the main directions for the development and application of network information technology. 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 management of smart cities, and smart hospitals and the upgrading and transformation of industrial production, and people's daily lives. It also provides new ways and technical support for solving many bottlenecks that restrict social and economic development.

The Internet of Things system structure mainly includes a 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 realization of the Internet of Things business, and the network layer mainly relies on various network forms to complete data interaction [1]. Specific to the actual application of the Internet of Things technology, its application system generally includes a central server, a monitoring center, a wireless transmission

How to cite this article (APA): Rao, B.B., and Woo, A.A. (2024). Implementing Token-Based Authentication and Modified Hashing for IoT Security. *ShodhKosh: Journal of Visual and Performing Arts, 5*(1), 502–512. doi: 10.29121/shodhkosh.v5.i1.2024.1880

network, a remote client, a server, various communication modules, and corresponding sensing devices. Its specific technical structure can be seen in Figure 1.

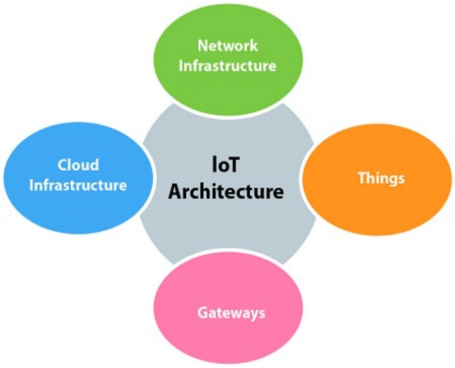


Figure 1: Technical Structure of the Internet of Things [2].

The structure of the Internet of Things system is more complex, and its functions are also different. We need to complete the collection, analysis, conversion, transmission, and control of data information according to its respective functions, to ensure that dynamic data can be efficiently and accurately connected with its corresponding equipment to complete the corresponding actions or tasks. There is a large amount of data interaction on the Internet of Things, and it needs to rely on the Internet to realize its various functions. As a consequence, the security issues of its data information and the stability and reliability of the Internet of Things operation have become the key content in the construction and management of the Internet of Things. The continuous development and popularization of network technology, not only brings convenience to people's lives but also increases data security risks.

In computer networks, the invasion of viruses and Trojan horses seriously threatens the security of the network environment. Hackers' attacks on the vulnerabilities of the Internet of Things system will also pose a huge threat to the stability of the Internet of Things and the security and confidentiality of data information on the Internet of Things [3]. Therefore, to ensure the information security of the Internet of Things, we must conduct a comprehensive analysis of various security risks and actively apply advanced data and information security protection technologies to enhance the ability of the Internet of Things to resist illegal intrusion. Only in this way can we give a dependable guarantee for the development and creation of the Internet of Things technology. Simultaneously, we must actively apply advanced encryption techniques and other automated and intelligent technologies in the construction of the Internet of Things to improve the information and intelligence of the Internet of Things, making it an important driving force for the development of the information industry. Some generally used security technologies in Internet of Things networks are:

A. Application of Security Risk Identification in the Internet of Things: Technicians must enhance their security risk awareness when erecting the Internet of Things, and establish a scientific and complete security risk identification system grounded on the characteristics of the Internet of Things. Technicians should conduct a comprehensive analysis of the various security risks that may exist on the Internet of Things, accurately calculate the risk level coefficients of different hidden dangers, and nicely determine the threat position norms to ameliorate the capability of the Internet of effects to identify security pitfalls. In the meantime, we should also apply security threat assessment throughout the entire process of IoT construction and operation.

B. Application of Control Security Technology in IoT Network: To ensure the security of the Internet of Things and improve the stability of the operation of the Internet of Things, we must actively apply advanced computer network control technology in the construction and management of the Internet of Things. Meanwhile, we should make a complete control system in the local area network to effectively prevent the Internet of Things from being threatened by viruses, Trojan horses, and hackers. In this way, the security of data information on the Internet of Things can also be guaranteed, so that the Internet of Things has a good operating terrain.

When applying network control technology to the Internet of Things, we can set a two-dimensional code to identify whether the communication operation behaviour of the Internet of Things is legal before connecting to the computer network, and corresponding isolation and blocking measures should be set for various illegal operations [4]. A specialized labour force should also strengthen the construction of the control system in the original area network of the Internet of Effects to help data leakage or data tampering after the Internet of Effects is obtruded with or raided.

C. Application of Communication Security Technology in IoT Network: Since the Internet of Things needs to be linked to a computer network during its operation; the openness of the computer network makes it a more security risk factor. Concurrently, the Internet of Things often has a lot of information interaction when it is running. As a consequence, we must ameliorate the mindfulness of IoT data security and ensure the confidentiality and security of data information in the IoT system through the operation of communication security technology. Illegal program code is an important factor that affects the effectiveness of IoT system control and data security. As a result, one must actively adopt corresponding security technologies to detect behaviors such as changing the message flow, forging initialization, and denying message services. Moreover, technicians must prevent the content of the message and communication volume of the Internet of Things communication system from being illegally analyzed by the outside [6]. Only in this way can the communication security of the IoT system be ensured, and illegal codes can be prevented from affecting the security of the IoT operation.

D. Application of Data Storage Security Technology in IoT Network: To improve the security of IoT data storage in the construction and management of the Internet of Things, we should ensure that its data storage space capacity can meet the actual needs of data storage. Otherwise, we should also strengthen the management of data and information, and improve the ability of the Internet of Things system to resist intrusion and damage through the application of information backup and self-repair technologies to ensure the safe operation of the Internet of Things. At the same time, in the construction of the Internet of Things, we should also actively apply isolation restriction technology to divide the Internet of Things into multiple relatively independent technical control areas. This is beneficial to enable them to effectively control the scope of data damage through system isolation restrictions in times when they are illegally invaded, and enhance their resistance to illegal intrusion behaviors, thereby preventing data in other units from being affected. Internet of Things (IoT) devices are operating in various domains like healthcare environments, smart cities, smart homes, transportation, and smart grid systems [58; 59; 60]. These biases transmit a bulk of data through sensor detectors, actuators, transceivers, or other wearable biases. Data in the IoT terrain is susceptible to numerous pitfalls, attacks, and pitfalls. Thus, a robust security medium is necessary to manage attacks, vulnerabilities, security, and sequestration challenges related to IoT.

2. INTERNET OF THINGS AND SECURITY OF DEVICES

Thanks to a plethora of new “smart” services and products, such as smart appliances, smart houses, smart watches, smart TVs, and so on, IoT devices are quickly spreading in all environments, becoming every day more pervasive. Moreover, many of such smart services require users to intentionally reveal some personal (and, sometimes, private) information in exchange for advanced and more personalized services. It's also clear that security and sequestration should be of primary significance in the design of IoT technologies and services. Unfortunately, this isn't the case for numerous IoT marketable products that are handed with shy, deficient, or ill-designed security mechanisms. In the last times, growing attention has been devoted to the pitfalls related to the use of simple IoT bios in services that have access to sensitive information or critical controls, such as video recording of private environments, real-time personal localization, health-monitoring, building access control, industrial processes, traffic lights [7], [8]. Furthermore, some security attacks against commercial IoT devices have appeared in the mass media, contributing to raising public awareness of the security threats associated with 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 [9]. However, the wide heterogeneity of IoT devices hinders the development of well-established security-by-design methods for the IoT [10], [11]. The severe limits in terms of energy, communication, calculation, and storehouse capabilities of numerous IoT devices further complicate the challenge. Such limits indeed prevent the possibility of adopting standard security mechanisms used in more traditional Internet-connected devices [12], and call for new solutions that, however, are not yet standardized.

Besides the technical aspects, it is also necessary to develop a cyber-security culture among the IoT stakeholders, in particular manufacturers and final users. 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). A similar bias was first designed to work in insulated systems, for which the security pitfalls are much more limited. As a consequence, numerous manufacturers don't retain solid moxie in cyber security and may be ignorant of the security pitfalls associated with connecting their devices to a global network. Such a lack of know- style, together with the excited approach to the design of new products and the need to compress costs and time- to- requests have led to the commercialization of IoT products where security is either neglected or treated as an afterthought [13]. In parallel, the final users are also not very educated in terms of security practices and often fail to implement even the most basic procedures to protect their devices, e.g., changing the pre-installed password of the devices on first use. Such an underestimation of their part in guarding particular devices makes users themselves ignorant and unintentional abettors of possible attackers.

A survey from the McKinsey Global Institute estimates investments in the Internet of Things (IoT) to be over $11 trillion by 2025 [14]. 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 [15], share access to sensitive information with other networking devices (e.g., servers and gateways) present in corporate networks and critical systems [16]– [21]. In these settings, hackers can impersonate licit IoT bias via spoofing attacks and gain unauthorized access to the networks. 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 [22]–[25]. 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 [26], [27]. 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 [28]. This fragile and simple structure of IoT makes it more vulnerable to 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 a smartphone, laptop, palmtop, etc. are more robust and efficient. These devices can be connected with IoT devices to secure them like a smartphone can be used as a controller home automation system and IoT devices can be authenticated by using a smartphone as a QR-code authenticator [29], [30]. Mobile devices can also be used as IoT middleware that is designed specifically for low-powered resource-constrained to process data easily from sensors [31]. 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 [32]. Mobile applications in the context of IoT management can play a vital role. The IoT devices' 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 [33]. Similarly, the current IoT devices available in the market with lousy security, leading to vulnerabilities that will ‘‘affect flesh and blood’’ [34]. We need some solutions to address these security and privacy risks.

3. RELATED WORKS

IoT devices are pervasive and ubiquitous as per the prediction the number of IoT devices to be 50 billion by 2020 [35]. 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 [36]. Strong security is a dire need of IoT due to the rapid rise in IoT devices and cyber-attacks [37]. 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 generalities 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.

Regular and organized approaches for security analysis of IoT are discussed Mohammadi et al. [38] performed SLR and presented trust-based IoT recommendation techniques. Bhandari and Gupta [39] performed a systematic review based on fault analysis of IoT. Fazal et al. [40] 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. [41] systematically analyzed the security issues of IoT based on different layers. Macedo et al. [42] conducted SLR to analyze the security based on four security aspects such as trust, access control, data protection, and authentication. Martinez et al. [43] highlighted threats, attacks, challenges, and countermeasures related to the security of IoT. Similarly, Witti and Konstantas [44] evaluated the existing security and privacy issues through a systematic mapping study. Sultan et al. [45] 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 shortcomings of these mechanisms adopted by the current Internet of Things security convergence algorithm, this paper [46] proposes a network security detection algorithm based on association rule mining. This algorithm avoids the frequency of IoT nodes based on the timestamp mechanism, improves the read-write conflict of IoT nodes, and improves the convergence 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 detection algorithms, and ameliorate the security of data transmission and storehouse in Internet of Things 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	Description
47/2019	AES Algorithm	Car Tracking System Using IoT	AES algorithm is proposed with the method of generating a dynamic key.
48/2019	elliptic curve cryptography	Hardware-accelerated DTLS for IoT Security.	Transport layer security (DTLS) protocol to enable end-to-end security for the Internet of Things (IoT).
49/2020	SHA-3 Algorithm.	SHA-3 Co-Processor in Field-Programmable Gate Array.	Implements an SHA-3 Co-Processor in FPGA suitable for IoT applications.
50/2020	Novel graphical security model to capture malware spread in IoT.	Graphical security mode for Mirai.	Investigate infection behaviors of Mirai and its variants to explore malware spreading in IoT networks.
51/2021	Grayscale using steganographic coding.	Secure implementation of data transmission in the IoT system	Secure transmission based on steganographic substitution by synthesizing digital sensor data.
52/2022	Rivest Cipher (RC6) and SHA-256.	Efficient access control mechanism for Internet of Medical Things-based health care system.	Rivest Cipher (RC6), is used to generate the key value, and the elliptic curve digital signature algorithm will encrypt the key value
53/2022	Improved elliptic curve digital signature algorithm	Industrial IoT Security.	Hybrid encryption encrypts and decrypts the edge data in IIoT.
54/2022	PKI digital certificate.	Certificate Authority (CA) for cloud IoT systems	Highly secure and robust authentication protocol based on a PKI digital certificate based on two Certificate Authority (CA) for cloud IoT systems.

55/2018	MQTT with Oauth, HOTP, and AES	Device-to-device communication	MQTT requires more memory and processing power, Limits scalability
56/2018	ECC	Cryptosystem	Complicated and tricky. It increases the size of the encrypted message.
57/2018	Secure Vaults with HMAC	Secure vault	Slower. Refreshment of a key is required.

4. PROPOSED SYSTEM

The proposed system architecture is shown below:

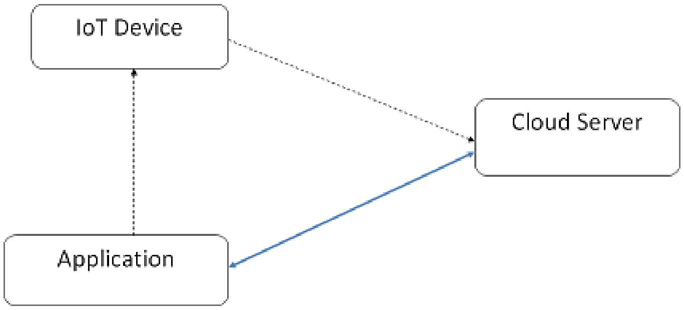


Figure 2: Proposed architecture.

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:

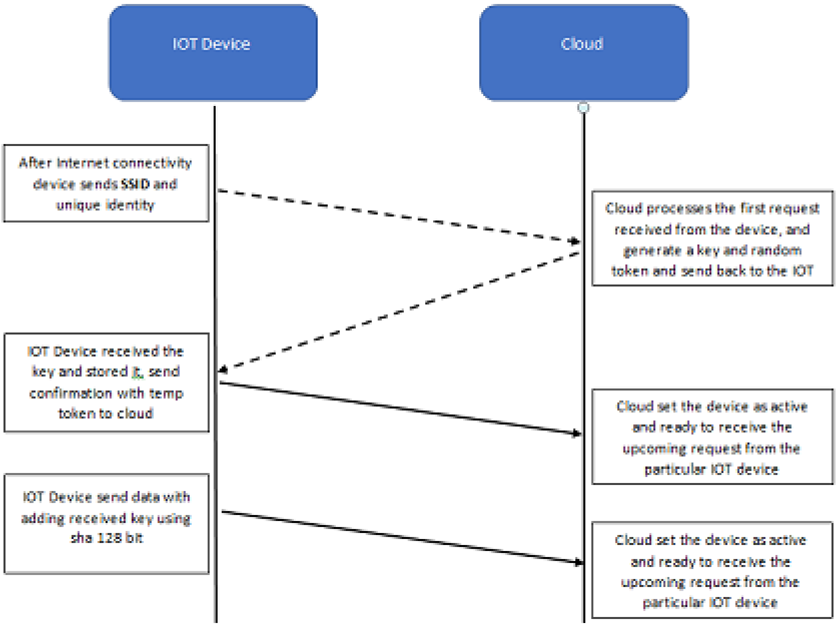

IOT Device
Cloud
After Internet connectivity device sends SSID and unique identity
Cloud processes the first request received from the device, and generate a key and random token and send back to the IOT
IOT Device received the key and stored it, send confirmation with temp token to cloud
Cloud set the device as active and ready to receive the upcoming request from the particular IOT device
IOT Device send data with adding received key using sha 128 bit
Cloud set the device as active and ready to receive the upcoming request from the particular IOT device

Figure 3: Proposed flow.

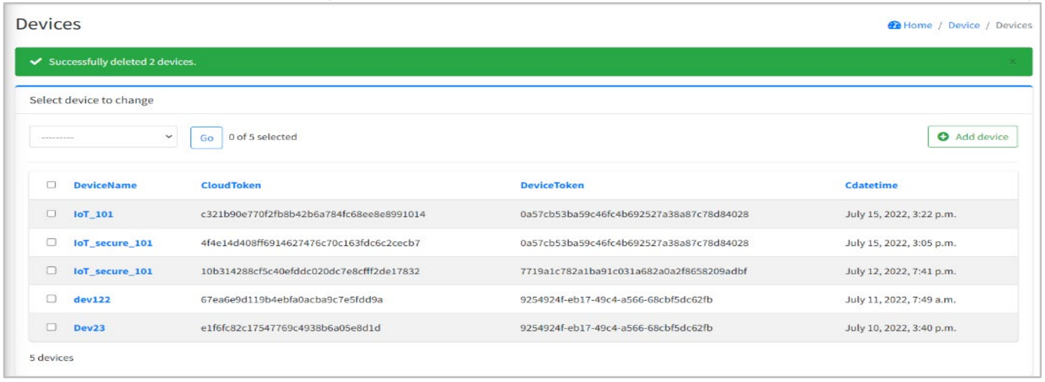
The algorithm for secure data communication between IoT devices and the cloud is as follows:

1. Start the 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 a 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 devices receive payload data extract it and save 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. A cloud receives hash then decodes with the same key and reads data.

5. RESULTS AND ANALYSIS

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



Devices

✓ Successfully deleted 2 devices.

Select device to change

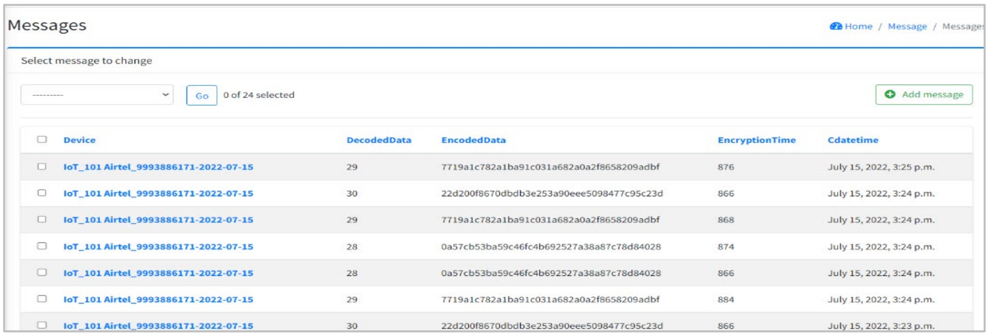
0 of 5 selected

□	DeviceName	CloudToken	DeviceToken	Cdatetime
□	IoT_101	c321b90e770f2fb8b42b6a784fc68ee8e8991014	0a57cb53ba59c46fc4b692527a38a87c78d84028	July 15, 2022, 3:22 p.m.
□	IoT_secure_101	4f4e14d408ff6914627476c70c163fdc6c2cecb7	0a57cb53ba59c46fc4b692527a38a87c78d84028	July 15, 2022, 3:05 p.m.
□	IoT_secure_101	10b314288cf5c40efddc020dc7e8cfff2de17832	7719a1c782a1ba91c031a682a0a2f8658209adbf	July 12, 2022, 7:41 p.m.
□	dev122	67ea6e9d119b4ebfa0acba9c7e5fdd9a	9254924f-eb17-49c4-a566-68cbf5dc62fb	July 11, 2022, 7:49 a.m.
□	Dev23	e1f6fc82c17547769c4938b6a05e8d1d	9254924f-eb17-49c4-a566-68cbf5dc62fb	July 10, 2022, 3:40 p.m.

5 devices

Figure 4: Device Token.

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



Messages

Select message to change

0 of 24 selected

□	Device	DecodedData	EncodedData	EncryptionTime	Cdatetime
□	IoT_101 Airtel_9993886171-2022-07-15	29	7719a1c782a1ba91c031a682a0a2f8658209adbf	876	July 15, 2022, 3:25 p.m.
□	IoT_101 Airtel_9993886171-2022-07-15	30	22d200f8670dbdb3e253a90eee5098477c95c23d	866	July 15, 2022, 3:24 p.m.
□	IoT_101 Airtel_9993886171-2022-07-15	29	7719a1c782a1ba91c031a682a0a2f8658209adbf	868	July 15, 2022, 3:24 p.m.
□	IoT_101 Airtel_9993886171-2022-07-15	28	0a57cb53ba59c46fc4b692527a38a87c78d84028	874	July 15, 2022, 3:24 p.m.
□	IoT_101 Airtel_9993886171-2022-07-15	28	0a57cb53ba59c46fc4b692527a38a87c78d84028	866	July 15, 2022, 3:24 p.m.
□	IoT_101 Airtel_9993886171-2022-07-15	29	7719a1c782a1ba91c031a682a0a2f8658209adbf	884	July 15, 2022, 3:24 p.m.
□	IoT_101 Airtel_9993886171-2022-07-15	30	22d200f8670dbdb3e253a90eee5098477c95c23d	866	July 15, 2022, 3:23 p.m.

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:

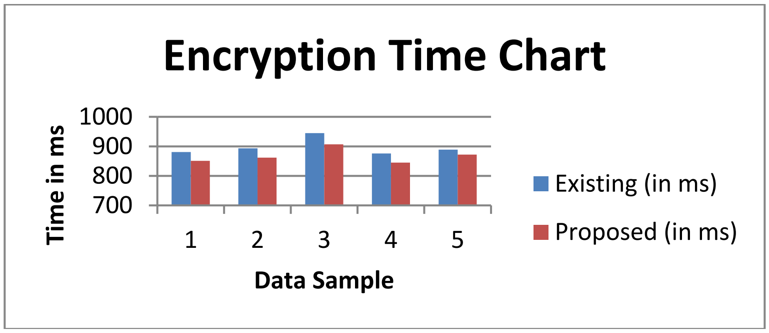


Figure 6: Comparison between existing and modified hash methods for encryption time.

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 in Table 2:

Table 2: Comparative with existing research

Method	Implementation	Complexity	Overhead	User anonymity	Prone to attack
[55]	Easier	High	More	Yes	Yes
[56]	Complex	High	More	Yes	Yes
[57]	Complex	High	More	Yes	Yes
Proposed	Easier	Low	Less	No	More enhanced

6. 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. It has been determined that the proposed system is more secure and less complex than the current system.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Wang Zhiqiang. Preliminary study on computer network security and remote-control technology of Internet of Things [J]. Electronic Testing, 2020(13): 96-97.

A. 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.

Wen Jinhui. Discussion on Internet of Things Computer Network Security and Its Remote-Control Technology [J]. Electronic Testing, 2020(10): 69-70.

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

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.

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

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.

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.

M. R. Warner, "Internet of Things Cybersecurity Improvement Act of 2017," S. 1691, 115th US Congress, Sep. 2017.

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.

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.

Y. B. Saied, "Collaborative security for the Internet of Things," Ph.D. dissertation, Institute National des Telecommunications, Jun. 2013.

C. 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.

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.

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

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, 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.

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.

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.

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

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

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

“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. 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.

L. Babun, A. K. Sikder, A. Acar, and A. S. Uluagac, “IoTDots: A Digital Forensics Framework for Smart Environments,” 2018. [Online]. Available:

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

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.

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.

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.

C. 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.

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

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.

R. Roman-Castro, J. Lopez, and S. Gritzalis, “Evolution and trends in IoT security,'' Computer, vol. 51, no. 7, pp. 16_25, 2018.

J. 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.

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

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.

V. Mohammadi, A. M. Rahmani, A. M. Darwesh, and A. Saha, “Trust-based recommendation systems in the Internet of Things: A systematic literature review,'' Hum. - Centric Comput. Inf. Sci., vol. 9, no. 1, p. 21, Dec. 2019.

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.

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

M. 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.

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.

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.

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.

A. 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.

G. 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.

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.

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.

I. 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.

D. 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.

A. 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.

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.

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.

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, *d*oi: 10.1109/JIOT.2022.3168726.

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.

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

Trusit Shah and S. Venkatesan, "Authentication of IoT Device and IoT Server Using Secure Vaults", IEEE, 2018.

Rao, BB., Waoo, AA., DESIGN A NOVEL APPROACH FOR TOKEN BASED AUTHENTICATION IN IOT NETWORKS, Ilkogretim Online - Elementary Education Online, Year; Vol 20 (Issue 4): pp. 2401-2406, http://ilkogretim-online.org, doi: 10.17051/ilkonline.2021.04.275

Rao, B.B., & Waoo, D.A. (2020). A TOKEN-BASED AUTHENTICATION SYSTEM THAT IDENTIFIES USERS AND DEVICE IN AN IOT APPLICATION/ECOSYSTEM, Volume 7, Issue 10, pp3066-3069

Tiwari, Anurag and Waoo, Akhilesh A., IoT based Smart Home Cyber-Attack Detection and Defense (2023). TIJER - International Research Journal | August 2023, Volume 10, Issue 8, Available at SSRN: https://ssrn.com/abstract=4537209