



# Token Based Authentication and Modified Hashing Approach to Improve the Security of Internet of Things Enabled Wireless Networks

**Dr. Jyoti Ranjan Mohanty**

*Department of Computer Science and Application, Odisha University of Agriculture and Technology, Bhubaneswar, Odisha, India*

**Dr. Manas Ranjan Mohapatra**

*Department of Computer Science, Banki Autonomous College, Cuttack, Odisha, India*

**Dr. Subhadra Mishra**

*Department of Computer Science and Application, Odisha University of Agriculture and Technology, Bhubaneswar, Odisha, India*

**Debaswapna Mishra**

*Department of Computer Science and Application, Odisha University of Agriculture and Technology, Bhubaneswar, Odisha, India*

**Janmejaya Sathua**

*Department of Computer Science, Nayagarh Autonomous College, Nayagarh, Odisha, India*

## ABSTRACT

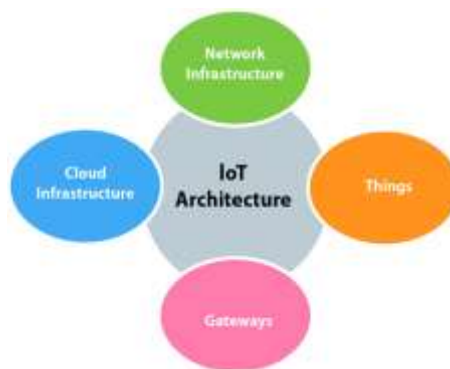
The concept of Internet of Things (IoT) is continuously evolving day to day and thus allowing various applications in different fields such as agriculture, education, industry, health, transportation etc. IoT being applied over these areas is influencing in a direct manner our lives, standing behind concepts like smart city, smart payment transfer, smart transportation, smart grid etc. In the IoT model, Internet-connected embedded devices perform manipulation on different sensitive data of users and need enough security solutions. The security solutions designed for network-enabled embedded devices must resolve issues like availability and usability, taking into account that IoT appliances require low computational capabilities and low consumption. It is difficult to implement IoT security solutions due to the factor that the newly purchased IoT devices are not equipped with a digital identity; therefore a user-friendly mechanism must handle the security material provisioning and attach the IoT device to the user cloud component account. This paper provides an in-depth literature review on IoT security issues and presented a modified hashing algorithm that is more efficient in device communication.

**KEYWORDS:** *IoT security, IoT device, AES, Token based authentication, SHA, Cloud, Modified hashing*

## 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 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 application of the Internet of Things technology will greatly promote the improvement of the degree of Informatization in related fields. In addition, it also has an important impact on the construction and management of smart cities, smart hospitals and the upgrading and transformation of industrial production, and people's daily lives. And it also provides new ways and technical

support for solving many bottlenecks that restrict social and economic development. In the Internet of Things system structure, it mainly includes 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 [50]. Specific to the actual application of the Internet of Things technology, its application system generally includes a central server, a monitoring centre, a wireless transmission 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 internet of Things [5].**

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 their respective functions, so as 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 in the Internet of Things, and it needs to rely on the Internet to realize its various functions. In

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. With the continuous development and popularization of network technology, it not only brings convenience to people's production and life, 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 in the Internet of Things [51]. Therefore, in order 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 provide a reliable guarantee for the development and promotion 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 commonly used security technologies in Internet of Things networks are:

#### **A. Application of Security Risk Identification in Internet of Things:**

Technicians must enhance their security risk awareness when building the Internet of Things, and establish a scientific and complete security risk identification system based on the characteristics of the Internet of Things. Technicians should conduct a comprehensive analysis of the various security risks that may exist in the Internet of Things, and accurately calculate the risk level coefficients of different hidden dangers, and reasonably determine the risk level standards to improve the ability of the Internet of Things to identify security risks. In the mean time, we should also implement security risk assessment throughout the entire process of IoT construction and operation management.

#### **B. Application of Control Security Technology in IoT Network:**

In order 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 build 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 in the Internet of Things can also be guaranteed, so that the Internet of Things has a good operating environment. When applying network control technology in 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 [22]. Technical personnel should also strengthen the construction of the control system in the local area network of the Internet of Things to prevent data leakage or data tampering after the Internet of Things is interfered or invaded.

#### **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 more security risk factors. Concurrently, the Internet of Things often has a lot of information interaction when it is running. As a consequence, we must improve the awareness of IoT data security and ensure the confidentiality and security of data information in the IoT system through the application 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 behaviours 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 [19]. 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:** In order 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 time when they are illegally invaded, and enhance their resistance to illegal intrusion behaviours, thereby preventing data in other units from being affected. Internets of Things (IoT) devices are operating in various domains like healthcare environment, smart cities, smart homes, transportation, and smart grid system. These devices transmit a bulk of data through various sensors, actuators, transceivers, or other wearable devices. Data in the IoT environment is susceptible

to many threats, attacks, and risks. Therefore, a robust security mechanism is indispensable to cope with attacks, vulnerabilities, security, and privacy challenges related to IoT.

### 1.1 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, the IoT devices are quickly spreading in all environments, becoming everyday more pervasive. Moreover, many of such smart services require users to intentionally reveal some personal (and, sometimes, private) information in change for advanced and more personalized services. It is then clear that security and privacy should be of primary importance in the design of IoT technologies and services. Unfortunately, this is not the case for many IoT commercial products that are provided with inadequate, incomplete, or ill-designed security mechanisms. In the last years, growing attention has been dedicated to the risks related to the use of simple IoT devices 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 accesses control, industrial processes, traffic lights [21], [43]. Furthermore, some security attacks against commercial IoT devices have appeared in the mass media, contributing to raise public awareness of the security threats associated with the IoT world.

In order 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 challenge is further complicated by the severe limits in terms of energy, communication, computation,

and storage capabilities of many IoT devices. Such limits indeed prevent the possibility of adopting standard security mechanisms used in more traditional Internet-connected devices [53], 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. As a matter of fact, many IoT device manufacturers come from the market of low-cost sensors and actuators (e.g., home automation, lights 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. As a consequence, many manufacturers do not possess a solid expertise in cyber security and may be unaware of the security risks associated with connecting their devices to a global network. Such a lack of know-how, together with the hectic approach to the design of new products and the need to compress costs and time-to-market have led to the commercialization of IoT products where security is either neglected or treated as an afterthought [9]. In parallel, the final users are also not much educated in terms of security practices and often fail to implement even the most basic procedures to protect their devices as, e.g., changing the pre-installed password of the devices on first use. Such an underestimation of their role in protecting personal devices makes users themselves unaware and unintentional allies 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 [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 [32],[31],[54],[55],[33]. In these settings, hackers can impersonate legitimate IoT devices 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 to 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 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 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. But, 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 analysing all the major threats, we integrated the Security in IoT system. The communication among the IoT devices is machine to machine (M2M) without the involvement of human. In hardware based solutions where only sensors, actuators and processors are used whereas security procedures and policies within smart phone, laptop, palmtop etc. is more robust and efficient. These devices can be connected with IoT devices to secure them like smart phone can be used as controller home automation system and IoT devices can be authenticated by using smart phone as QR-code authenticator [52], [37]. The 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, the mobile applications and IoT will be the most disruptive class of technologies in the next 10 years [16]. The mobile applications in 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 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 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.

## 2. RELATED WORKS

IoT devices are pervasive and ubiquitous in nature as per predication the number of

IoT devices to be 50 billion by 2020 [24]. With rise of this mammoth elevation in number, security has become burning issue and has grabbed a great deal of attention in last few years. Security is important from device to device as it deals with the end-to end communication between individual devices [13]. The strong security is the 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 systematic approach has been performed by different authors with different aspects but the main focus of this research work is to analyse the security of IoT by using the concepts of mobile computing. The security analysis of IoT by using mobile computing is novel approach and it is the first attempt to analyse the security of IoT devices in light of mobile computing.

Systematic approaches for security analysis of IoT are discussed like Mohammadi et al. [47] performed SLR and presented trust based IoT recommendation techniques. Bhandari and Gupta [18] performed a systematic review based upon fault analysis of IoT. Fazal et al. [29] analysed the security of IoT through systematic approach and they focused upon highlighting and classifying the security challenges at three different aspects such that hardware, network and cloud server. Aly et al. [34] systematically analysed the security issues pertaining to IoT based upon different layers. Macedo et al. [14] conducted SLR to analyse the security based upon four security aspects such as trust, access control, data protection, and authentication. Martinez et al. [27] highlighted threats, attacks, challenges and countermeasures related to security of IoT. Similarly, Witt and Konstantas [38] evaluated the existing security and privacy issues by systematic mapping study. Sultan et al. [4] analysed the security issues and provided the solution by using block chain 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 life. The development of network technology further promotes the development of Internet of Things technology based on it. The development of the Internet of Things has greatly improved the efficiency and convenience, but at the same time, there are many security risks. In view of the shortcomings of these mechanisms adopted by the current Internet of Things security convergence algorithm, this paper [17] proposes a network security detection

algorithm based on association rule mining. This algorithm avoids the frequency of IoT nodes based on timestamp mechanism, improves the read-write conflict of IoT nodes, and improves the convergence rate of network security. And it can meet the online security detection and analysis of large-scale networks, effectively solve the defects of current network security detection algorithms, and improve the security of data transmission and storage in Internet of Things applications.

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

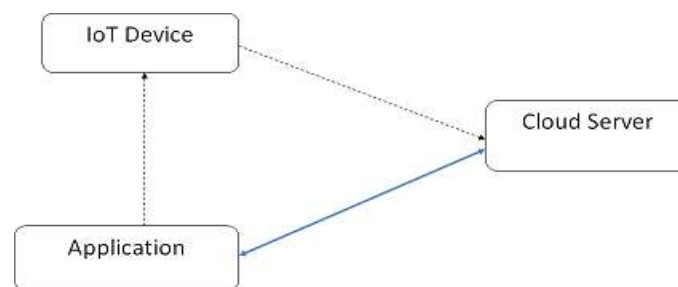
**Table 1: Major research in the field**

Ref./Year	Techniques Used	Application	Description
[44]/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).
[23]/2020	SHA-3 Algorithm.	SHA-3 Co-Processor in Field-Programmable Gate Array.	Implements a SHA-3 Co-Processor in FPGA suitable for IoT applications.
[12]/2020	Novel graphical security model to capture malware spread in IoT.	Graphical security mode for Mirai.	Investigate infection behaviours of Mirai and its variants to explore malware spreading in IoT networks.
[3]/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.
[42]/2022	Rivest Cipher (RC6) and SHA-256.	Efficient access control mechanism for Internet of Medical Things-based health care system.	Rivest Cipher (RC6), are used to generate the key value, and elliptic curve digital signature algorithm will encrypt the key value
[57]/2022	Improved elliptic curve digital signature algorithm	Industrial IoT Security.	Hybrid encryption to encrypt and decrypt the edge data in IIoT.
[56]/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.
[39]/2018	MQTT with Oauth, HOTP and AES	Device to device communication	MQTT requires more memory and processing power, Limits scalability
[15]/2018	ECC	Cryptosystem	Complicated and tricky. It increases the size of encrypted message.
[45]/2018	Secure Vaults with HMAC	Secure vault	Slower. Refreshment of key is required.

### 3. PROPOSED SYSTEM

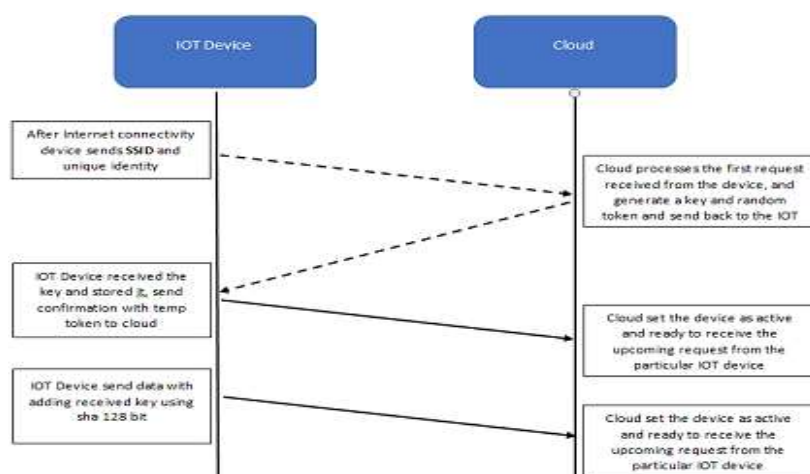
Proposed system architecture is shown below:



**Figure 2: Proposed architecture.**

In the proposed system, there will be three modules, IoT device, Cloud Server, and application. The IoT device will be a wearable IoT device. 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. Diagram below shows flow of the proposed system:



**Figure 3: Proposed flow.**

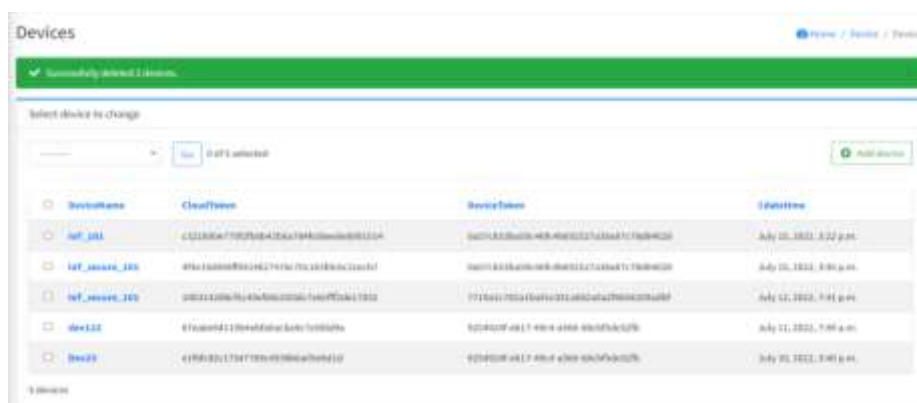


Algorithm for secure data communication between IoT device and cloud is as follows:

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 device sending payload to our cloud system and cloud recognized the IoT device.
7. Cloud system checks the IoT device entry in the database. Whether it is available or not if available then respond unique payload to an IoT device.
8. IoT device received 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 cloud: first get the value from the sensor then add modified hash with the stored token received from the cloud and send to the cloud.
11. Cloud received has, then decode with the same key and read data.

#### 4. RESULTS

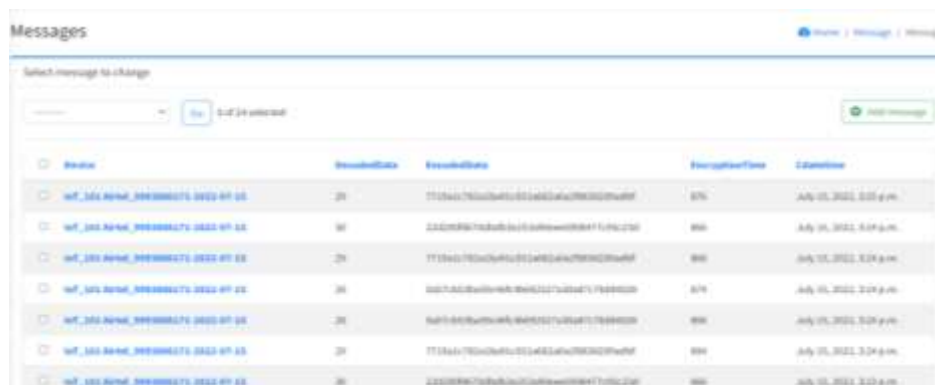
The proposed system has designed a token based authentication system that identifies user and device. The research had also design and modifies a secure Hashing Solution. System has device tokens shown in figure below:



DeviceName	CloudToken	DeviceToken	LastTime
IoT_001	42222222222222222222222222222222	42222222222222222222222222222222	July 10, 2022, 3:22 p.m.
IoT_device_101	42222222222222222222222222222222	42222222222222222222222222222222	July 10, 2022, 3:40 p.m.
IoT_device_102	42222222222222222222222222222222	42222222222222222222222222222222	July 11, 2022, 9:41 p.m.
IoT_103	42222222222222222222222222222222	42222222222222222222222222222222	July 11, 2022, 9:40 a.m.
IoT_104	42222222222222222222222222222222	42222222222222222222222222222222	July 10, 2022, 3:40 p.m.

**Figure 4: Device token.**

Snapshot of data received from IoT device is shown below:

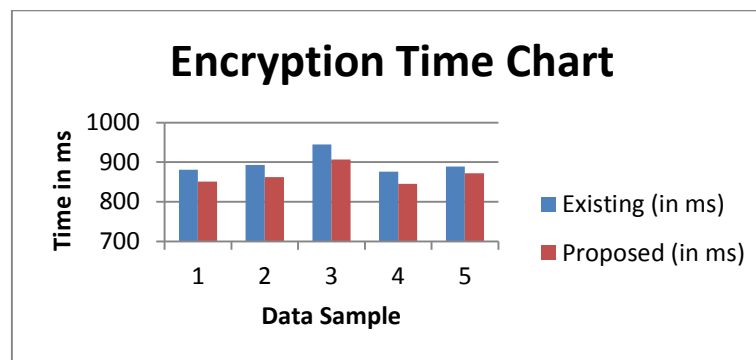


DeviceName	ReceivedData	EncodedData	ReceivedTime	LastTime
IoT_001	42222222222222222222222222222222	42222222222222222222222222222222	July 10, 2022, 3:22 p.m.	July 10, 2022, 3:22 p.m.
IoT_001	42222222222222222222222222222222	42222222222222222222222222222222	July 10, 2022, 3:40 p.m.	July 10, 2022, 3:40 p.m.
IoT_001	42222222222222222222222222222222	42222222222222222222222222222222	July 11, 2022, 9:41 p.m.	July 11, 2022, 9:41 p.m.
IoT_001	42222222222222222222222222222222	42222222222222222222222222222222	July 11, 2022, 9:40 a.m.	July 11, 2022, 9:40 a.m.
IoT_001	42222222222222222222222222222222	42222222222222222222222222222222	July 10, 2022, 3:40 p.m.	July 10, 2022, 3:40 p.m.
IoT_001	42222222222222222222222222222222	42222222222222222222222222222222	July 10, 2022, 3:40 p.m.	July 10, 2022, 3:40 p.m.

**Figure 5: Data received from IoT device.**

Proposed system has modified existing SHA method. Result below shows

comparison of SHA and modified SHA used in proposed system:



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

## 5. CONCLUSION

Improving security and reducing risks in information systems depend heavily on analysing threats, risks, and vulnerabilities to develop the appropriate counter measures 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.

Proposed system has been found more secure and less complex. We have analysed 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

## REFERENCES:

1. "Method of Resource-limited Device and Device Class Identification Using System and Function Call Tracing Techniques, Performance, and Statistical Analysis," Patent 10 242 193.
2. K. Sikder, L. Babun, H. Aksu, and A. S. Uluagac, "Aegis: A Context Aware Security Framework for Smart Home Systems," ser. ACSAC 2019.
3. Kabulov, I. Saymanov, I. Yarashov and F. Muxammadiyev, "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.
4. 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.
5. 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.
6. Babun, Leonardo, Aksu, Hidayet, Uluagac, S. A., "Detection of Counterfeit and Compromised Devices Using System and Function Call Tracing Techniques," Patent 10 027 697.
7. 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.
8. Kaygusuz, L. Babun, H. Aksu, and A. S. Uluagac, "Detection of Compromised Smart Grid Devices with Machine Learning and Convolution Techniques," in 2018 ICC.
9. Koliass, 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.
10. 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.
11. 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.
12. 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.
13. Buenrostro, D. Cyrus, T. Le, and V. Emamian, "Security of IoT devices," J. Cyber Secur. Technol., vol. 2, no. 1, pp. 1\_13, 2018.
14. 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.
15. E.H. Teguig& Y. Touati, "Security in Wireless Sensor Network and IoT: An Elliptic Curves Cryptosystem based Approach", IEEE, 2018
16. 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.
17. 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.
18. 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.
19. GuoJinhua, Ming Xiaobo. "Internet of Things Computer Network Security and Remote Control Technology", [J]. Contemporary Educational Practice and Teaching Research, 2016(3):264.
20. Aksu, L. Babun, M. Conti, G. Tolomei, and A. S. Uluagac, "Advertising in the IoT Era: Vision

- and Challenges,” IEEE Communications Magazine, 2018.
21. H. Almuhammedi, 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.
  22. Han Junfeng, “Analysis of Internet of Things Computer Network Security and Remote Control Technology” [J]. China New Communications, 2019, 21(21): 160.
  23. 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.
  24. 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.
  25. J. D. Fuller and B. W. Ramsey, “Rogue Z-Wave Controllers: A Persistent Attack Channel,” in 2015 LCN Workshops, 2015.
  26. 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.
  27. 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.
  28. 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.
  29. 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.
  30. 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>.
  31. 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.
  32. L. Babun, H. Aksu, and A. S. Uluagac, “Identifying Counterfeit Smart Grid Devices: A Lightweight System Level Framework,” in 2017 ICC, May 2017.
  33. 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>.
  34. 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.
  35. 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.
  36. M. R. Warner, “Internet of Things cybersecurity improvement act of

- 2017,” S. 1691, 115th US Congress, Sep. 2017.
37. 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.
  38. M. Wittl 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.
  39. 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.
  40. 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.
  41. R. Roman-Castro, J. Lopez, and S. Gritzalis, “Evolution and trends in IoT security,” *Computer*, vol. 51, no. 7, pp. 16\_25, 2018.
  42. 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.
  43. 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.
  44. 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.
  45. Trusit Shah and S. Venkatesan, “Authentication of IoT Device and IoT Server Using Secure Vaults”, IEEE, 2018
  46. 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.
  47. 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.
  48. 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.
  49. 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.
  50. Wang Zhiqiang. Preliminary study on computer network security and remote control technology of Internet of Things [J]. *Electronic Testing*, 2020(13): 96-97.
  51. Wen Jinhui. Discussion on Internet of Things Computer Network

- Security and Its Remote Control Technology [J]. *Electronic Testing*, 2020(10): 69-70.
52. 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.
53. Y. B. Saied, "Collaborative security for the Internet of Things," Ph.D. dissertation, Institute National des Telecommunications, Jun. 2013.
54. 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.
55. 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*.
56. 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.
57. 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.