



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY




INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Special Issue 1, April 2023

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

 9940 572 462

 6381 907 438

 ijrset@gmail.com

 www.ijrset.com

Analysis of Data Security and Privacy in Cloud Based Internet of things Network

M. Jeevan Kumar¹, Dr. Vishal Bhatnagar²

Research Scholar, Department of C.S.E, Shri Venkateshwara University, Gajraula, Uttar Pradesh, India¹

Research Guide, Department of C.S.E, Shri Venkateshwara University, Gajraula, Uttar Pradesh, India²

ABSTRACT: The Internet of Things (IoT) is an extensive and rapidly growing technology. Due to its networked nature and rapid implementation in various fields, security and privacy are considered as primary challenges. Due to various security vulnerabilities, IoT based infrastructure is prone to numerous security threats which in turn affect infrastructure on a wider scale. Users can communicate and use IoT devices via cloud component. This paper presents, Analysis of data security and privacy in Cloud based Internet of Things Network. It emphasizes the collection of (security) data from different elements of IoT systems, including individual devices and smart objects. This analysis is an extensible approach to modeling security data from a variety of IoT systems and devices. When communicating with cloud service, proper device access control is required. This approach enables the instantiation and deployment of security and privacy data collection systems over complex IoT networks. This analysis represents a way to authenticate both the IoT device and the user through a cloud system. Confidentiality, Integrity, Availability and Privacy percentages are defined parameters for performance analysis. Finally, we evaluated described model achieves high Confidentiality, Integrity, Availability which declares the security of model and privacy than normal IoT network.

KEYWORDS: Internet of Things (IoT), Cloud service, Cloud Storage, access control, Security and Privacy.

I. INTRODUCTION

IoT is an interconnection of everyday objects in a network, which are usually equipped with tremendous intelligence level. IoT has increased the usage of Internet gigantically by integrating every object for interaction through embedded systems, which leads to a highly dispersed network of devices communicating with human beings as well as electronic devices which support internet [1]. IoT is a promising phenomenon which will improve the quality of our lives. In the recent past, IoT has been the center of attraction of researchers and practitioners from all over the world [2]. IoT is a device which is capable of capturing data, storing and processing it. It can also visualize services, monitor and manage various devices [3].

IoT (Internet of Things) deployers are confronted with pressing security challenges, including more vulnerabilities and security attacks. The latter require new and more intelligent approaches to IoT security, notably approaches that are able to tackle complex, unpredictable and sometimes asymmetric attacks at scale [4]. There is a need of an advanced prototype for security, which considers the security issues from a holistic perspective comprising the advanced users and their inter communication with this technology [5]. Internet is primary of IoT hence there can be security loophole. Inter communication paradigms are developed based on sensing programming for IoT applications, evolving an intercommunication stack to develop the required efficiency and reliability. Securing intercommunication is a crucial issue for all the paradigms that are developing based on sensing programming for IoT applications [6].

IoT devices Security issues should be discussed from the manufacturing to IoT technology implementation Three components need to be addressed as IoT security concerns; Networks, applications and IoT devices [7]. For instance, because of incorrect configuration or vulnerabilities, IoT devices may be compromised. Security challenges need to be addressed strategically to find effective solutions [8]. Security in the IoT system should be built in. IoT devices are made unfortunately without focus on security concerns. In IoT, privacy is one of the primitive considerations for the

protection of information of individuals from exposure in the IoT environment, in which almost any physical or logical entity has been assigned a unique identifier and the ability to communicate autonomously over the Internet or similar network [9].

Based on various studies, these security risks were not considered as one of the primary concerns of many vendors and were not handled appropriately [10]. A Few of the major developments to solve these security issues are encryption mechanism or cryptography, authentication mechanism and access control technology [11]. Low-end IoT devices are incapable of performing heavier, conventional cryptographic algorithms due to their constrained resources [12]. A large quantity of IoT devices adopt wireless as a means to communicate, which is open to eavesdropping and jamming [13].

This paper presents Analysis of data security and privacy in Cloud based Internet of Things Network. It emphasizes the collection of (security) data from different elements of IoT systems, including individual devices and smart objects. The overall analysis provides the means for end-to-end security and privacy monitoring of an IoT network, including protection for all functional blocks and end points that it comprises. To this end, this analysis provide the means for identifying and anticipating attacks on internet-connected devices, including smart objects with dynamic behaviour.

The rest of the paper is organized as follows: Section II discussed some related literature survey, Section III presents Analysis of data security and privacy in Cloud based IoT Network. Section IV presents result analysis and finally paper concluded with Section V.

II. LITERATURE SURVEY

In [14] pointed out that some old techniques are no longer useful such as Snort, and other intrusion detection algorithms. Because IoT is somewhat different than conventional networks, modern tactics must be adopted to secure these widespread open architectures. In [15] propose the on-demand security configuration technique that we can configure required security functions and reorganize them without recreating device image. The advent of IoT which has vast amount of connected devices enables us to monitor and control of real world and changes our daily lifestyle never available before. With such a massive amount of devices, if we don't set and organize security features on them properly, we will face inexperienced challenges on security issues. With the help of this approach, if there is a change on this security service, we can substitute the old modules for new ones without regenerating device image.

In [16] enables the trust evaluation of cloud services in order to ensure the security of the cloud-based IoT context via integrating security- and reputation-based trust assessment methods. The security-based trust assessment method employs the cloud-specific security metrics to evaluate the security of a cloud service. The experiments conducted using a synthesized dataset of security metrics and a real-world web service dataset show that our proposed trust assessment framework can efficiently and effectively assess the trustworthiness of a cloud service while outperforming other trust assessment methods.

In [17] presents dynamic defense architecture for the security of IoT. It is made up of six security defense segments which include active defense, threat detection, security warning, security response, security recovery and defense assessment. The whole procedure of security defense repeats all along. The next segment provides supplements to the previous segment. IoT security threats are dealt with dynamically. According to operation results of all defense segments, the security situation of IoT is assessed, and then defense strategies for IoT are updated to make the proposed architecture adapt to the IoT environment.

In [18], we construct a new Ciphertext-policy attribute-based encryption (CP-ABE)-based storage model for data storing and secure access in a cloud for IoT applications. Our new framework introduces an attribute authority management (AAM) module in the cloud storage system functioned as an agent that provides a user-friendly access control and highly reduces the storage overhead of public keys. The analysis and simulation results demonstrate that our SEM-ACSIT scheme achieves powerful security with less computational overhead and lower storage costs than the existing schemes.

International Journal of Innovative Research in Science, Engineering and Technology*An ISO 3297: 2007 Certified Organization**Volume 12, Special Issue 1, April 2023***10th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '23)****5th -6th April 2023****Organized by****Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India**

In [19] introduces a multi-hop routing protocol that enables secured IoT devices' communication. The routing protocol enables the IoT devices to authenticate before forming a new network or joining an existing network. The proposed routing protocol embeds the multi-layer parameters into the routing algorithm, thus combining the authentication and routing processes without incurring significant overheads. The multi-layer parameters include a unique User-Controllable Identification, users' pre-agreed application(s), and a list of permitted devices, thus saving resources by maintaining smaller routing information. Experimental and field tests were conducted with results showing that our secure multi-hop routing is suitable to be deployed for IoT communication.

In [20] address the conflict in the collection, use, and management of Big Data at the intersection of security and privacy requirements and the demand of innovative uses of the data. This problem is exaggerated in the context of the Internet of Things (IoT). By identifying these distinct objectives for the design of IoT Big Data management, we propose that more effective design and control is possible at the intersection of these forces, through an iterative process of review and redesign.

In [21], the four layers of IoT are application, access gateway, internet, and the edge technology layer. These four layers make up the open network of IoT. However, others break down the layers into three, the internet, application, and perception layer. For this research, we consider the three-layered IoT architecture layout.

In [22] propose a new secure data search and sharing scheme for Cloud-edge-collaborative storage (CECS). Our scheme improves the existing secure CECS scheme in the following two ways. First, it enables users to generate a public-and-private key pair and manage private keys by themselves. Second, it uses searchable public-key encryption to achieve more secure, efficient, and flexible data searching. In terms of performance, the experimental results show that our scheme significantly reduces users' computing costs by delegating most of the cryptographic operations to edge servers. Especially, our scheme reduces the computing and communication overhead for generating a search trapdoor compared with the existing secure CECS scheme.

In [23] present a recommendation tool that models IoMT concepts and security issues in addition to successively recommending security measures. The presented tool utilizes semantically enriched ontology to model the IoMT components, security issues, and measures. We have experimented the proposed tool with respect to the completeness and effectiveness of its output (i.e., security issues and recommended security measures). The results show that the tool was effectively able to recommend necessary security measures.

In [24] propose and analyze a 3-tier cloud-cloudlet-device hierarchical trust-based service management protocol called IoT-HiTrust for large-scale mobile cloud Internet of Things (IoT) systems. The results demonstrate that IoT-HiTrust outperforms contemporary distributed and centralized trust-based IoT service management protocols in selecting trustworthy nodes to maximize application performance, while achieving scalability.

In [25] propose an innovative security testbed framework targeted at IoT devices. The security testbed is aimed at testing all types of IoT devices, with different software/hardware configurations, by performing standard and advanced security testing. The testbed operation is demonstrated on different IoT devices using several specific IoT testing scenarios. The results obtained demonstrate that the testbed is effective at detecting vulnerabilities and compromised IoT devices.

III. DATA SECURITY AND PRIVACY IN CLOUD BASED IOT NETWORK

The block diagram of Analysis of data security and privacy in Cloud based Internet of Things Network is represented in below Figure 1.

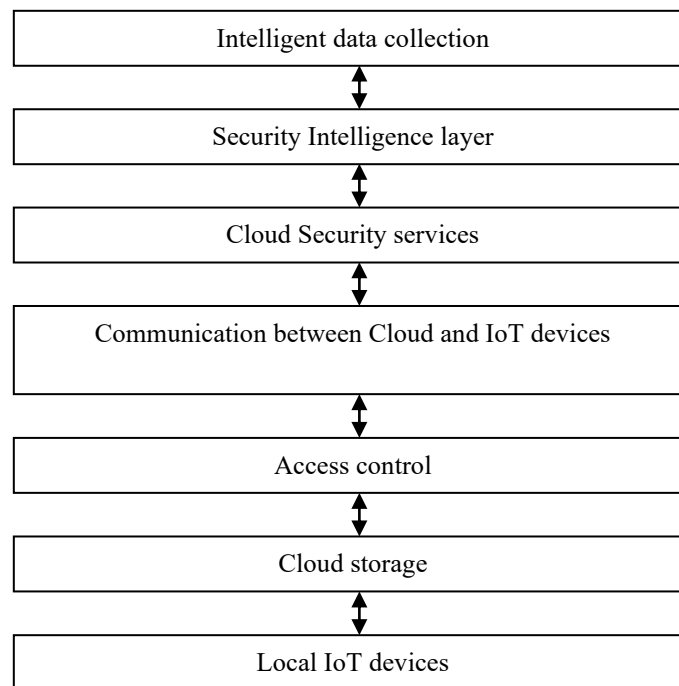


Figure 1. Block diagram of Data Security and Privacy in Cloud Based IoT Network

Various elements of IoT systems can act as sources of security information. The elements may be deployed on different IoT platforms and span multiple administrative domains. Data collection is in charge of interacting with the field for two purposes: (i) collecting security related data from the above-listed elements through various probes, and (ii) driving security related automation and actuation tasks such as the configuration of the security properties of IoT systems.

Security Intelligence layer analyses the collected data in order to identify security-related events and indicators in the form of incidents, threats and attacks. It is characterized as an “intelligence” layer, because it is the place where intelligent reasoning over the security context takes place by means of data analytics techniques. Security management agents provide the means for interacting with field IoT systems and devices for the purpose of implementing automation and actuation functions related to security.

Cloud security service layer comprises security as a service that are provided by the Secure IoT network platform, including Risk Assessment (RA) services, Compliance Auditing (CA) services and Developer Support (DS) services. This layer implements also other services that are based on the data processing outcomes of the Security Intelligence layer, such as alerting and visualization services.

IoT devices communicate directly with the cloud, the cloud itself should be properly protected. Communication between IoT devices and cloud should therefore be secured and authentic. When communicating with cloud service, proper device authentication is required. When devices and cloud use a weak form of authentication, the device identity could be used by a third party. Without a strong encryption process in place, the intruder will be able to obtain access to sensitive data during communication with the cloud. There should be a protection against man in the middle attack that can also intercept the IoT traffic. There should also be a protection against playback attack, which can cause an unauthorized action against cloud services or device. These problems can be mitigated by using strong authentication mechanism with cloud to protect against misidentification of device. Strong encryption can protect data from unauthorized access during the communication.

International Journal of Innovative Research in Science, Engineering and Technology*An ISO 3297: 2007 Certified Organization**Volume 12, Special Issue 1, April 2023***10th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '23)****5th -6th April 2023****Organized by****Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India**

Local cloud storage refers to a local data store that provides persistence for the information. It is characterized as “edge” or “local” data store as it is meant to store information close to the field and is distinguished from information that is stored at the cloud level. Local storage of security data can facilitate security intelligence. Note that the analysis of information at the local storage, may involve different types of analytics, but typically involves streaming analytics.

IoT systems consist of IoT devices connected through a network. Many local devices are available in markets depending on the usage such as security alarms, smart thermostats, smart locks, smart IP cameras, smart energy management devices, smart electricity meters, smart home appliances, smart health sensors, voice detectors and many more. These devices are connected to the backend servers or cloud service providers; data from these smart devices is collected and stored over the cloud. Therefore, users can access these devices directly or through the cloud.

The analysis of IoT security can provide good understanding for network operations. Another aspect in IoT security is that most IoT devices come in such conditions that no one can add security features. Therefore, security should come with IoT device as a built-in feature. IoT devices should also execute secured signed code authorized to run on devices, while being secured during run time. It is important to ensure that malicious attacks do not overwrites the code that should not be tampered with after being signed.

IV. RESULT ANALYSIS

This section presents the performance of described Cloud based IoT network model in terms of performance parameters as Security and Privacy. The conventional IT (Information Technology) security requirements need to be addressed by any security design, mainly known as the CIA (Confidentiality, Integrity and Availability) triad. A secure system is one that satisfies all the above requirements, while any action that poses threats to one or more of the requirements constitutes a security attack. The Cloud based IoT network Model is a specification of the different types of data that are collected, streamed, stored and processed by the IoT network platform. The purpose of the Data Model is to provide a common specification to all parts of the Cloud based IoT network platform for the different types of data that may be exchanged between them.

- 1) Confidentiality involves implementing some set of controls that restrict unauthorized access to some information, ensuring access rights and other privileges over data are obtainable only to users with valid permission throughout a process.
- 2) Integrity entails ensuring the accuracy, correctness and validity of data at the source, through communication networks and destination by protecting the data from tampering or modification by unauthorized persons.
- 3) Availability is making data and all other system resources or services readily obtainable by authorized users, services or applications whenever requested. This is particularly important in IoT since a number of services occur in real-time.
- 4) Privacy on the other hand typically involves the protection of personal data against unauthorized access.

Below Table 1 shows the Comparative performance analysis of described Cloud based Internet of Things Network and normal IoT network in terms of Confidentiality, Integrity, Availability and Security. Figure 2 denotes the Confidentiality parameter Comparative analysis between described Cloud based IoT Network and normal IoT network. It is clear that, Confidentiality of Cloud based IoT network is high compared to normal IoT network. In this X-axis denotes network models and Y-axis denoted Percentage value.

Table 1. Comparative performance analysis

Parameters	Cloud based IoT network	Normal IoT network
Confidentiality (%)	98	81
Integrity (%)	98	82
Availability (%)	97	83
Privacy (%)	97.5	80

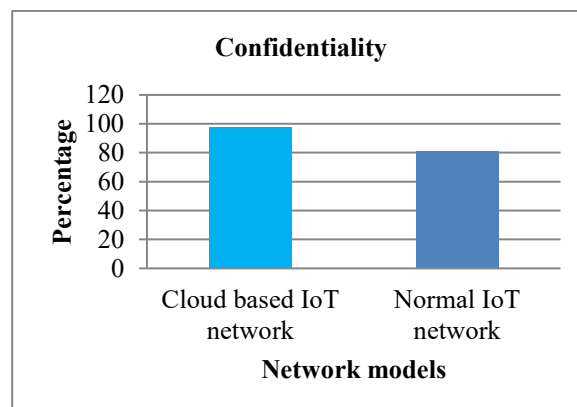


Figure 2. Confidentiality parameter Comparative analysis

Figure 3. Shows the graphical representation of performance of two networks in terms of Integrity, In which X-axis denotes network models and Y-axis denoted Percentage value. Integrity parameter percentage value is high for Cloud based IoT network compared to normal IoT. Graphical representation of Availability parameter for Cloud based IoT network compared to normal IoT is described in below Figure 4, and it states that, percentage Availability parameter is high for Cloud based IoT network. Y-axis denoted Percentage and X-axis denotes network models.

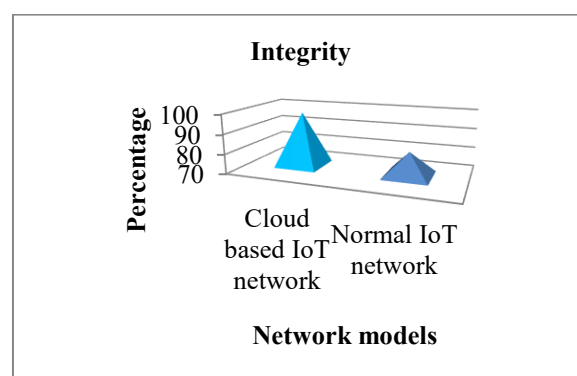


Figure 3. Integrity parameter Comparative analysis

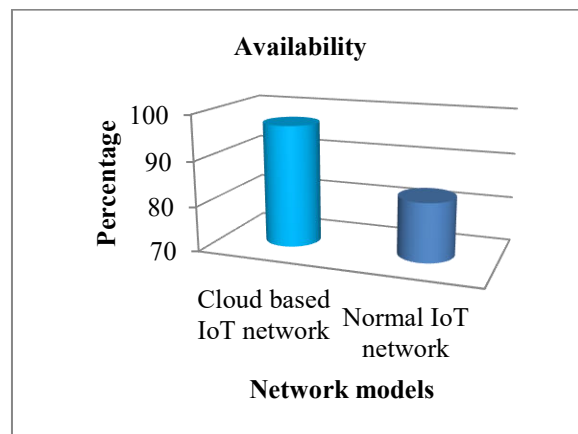


Figure 4. Comparative analysis for Availability parameter

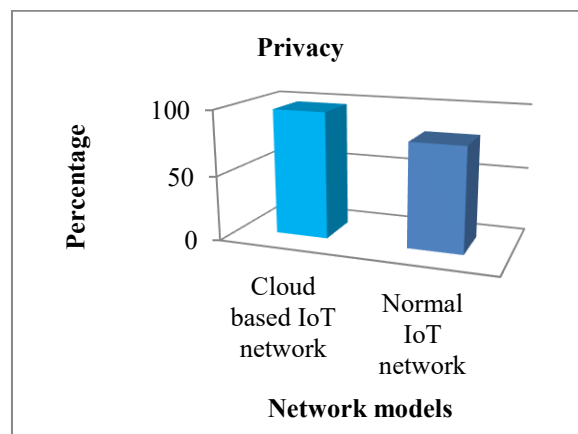


Figure 5. Comparative analysis for Privacy parameter

Comparative graphical representation of Privacy parameter for two networks in terms of Privacy parameter is represented in above Figure 5. In this Graph, Y-axis denoted Percentage and X-axis denotes network models. From graph it is clear that, Privacy of described model is high for Cloud based IoT network.

From overall results it is clear that, Analysis of data security and privacy in Cloud based Internet of Things Network is efficiently described the data security and privacy. Achieved values for described Cloud based IoT network are Confidentiality as 98%, Integrity as 98%, Availability as 97% and Privacy as 97.5%.

V. CONCLUSION

In this paper, Analysis of data security and privacy in Cloud based Internet of Things Network is represented. Security framework helps in understanding and minimizing security threats of IoT system. Described model emphasizes the collection of (security) data from different elements of IoT systems, including individual devices and smart objects. This analysis is an extensible approach to modeling security data from a variety of IoT systems and devices. Security Intelligence layer analyses the collected data in order to identify security-related events and indicators in the form of incidents, threats and attacks. This analysis represents a way to authenticate both the IoT device and the user through a

cloud system. Finally, we evaluated described Cloud based IoT network model achieves high Confidentiality, Integrity, Availability which declares the security of model and privacy than normal IoT network. Achieved values for described Cloud based IoT network are Confidentiality as 98%, Integrity as 98%, Availability as 97% and Privacy as 97.5%.

REFERENCES

- [1] Malti Bansal, Samarth Garg, "Internet of Things (IoT) based Assistive Devices", 2021 6th International Conference on Inventive Computation Technologies (ICICT), Year: 2021
- [2] K. M. Beshar, Z. Subah and M. Z. Ali, "IoT Sensor Initiated Healthcare Data Security," in *IEEE Sensors Journal*, vol. 21, no. 10, pp. 11977-11982, 15 May15, 2021, doi: 10.1109/JSEN.2020.3013634
- [3] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, "Anatomy of Threats to the Internet of Things," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1636-1675, Secondquarter 2019, doi: 10.1109/COMST.2018.2874978.
- [4] T. A. Ahanger and A. Aljumah, "Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms," in *IEEE Access*, vol. 7, pp. 11020-11028, 2019, doi: 10.1109/ACCESS.2018.2876939.
- [5] J. Wang *et al.*, "IoT-Praetor: Undesired Behaviors Detection for IoT Devices," in *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 927-940, 15 Jan.15, 2021, doi: 10.1109/JIOT.2020.3010023.
- [6] O. Arias, J. Wurm, K. Hoang and Y. Jin, "Privacy and Security in Internet of Things and Wearable Devices," in *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 99-109, 1 April-June 2015, doi: 10.1109/TMSCS.2015.2498605.
- [7] A. Mukherjee, "Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints," in *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747-1761, Oct. 2015, doi: 10.1109/JPROC.2015.2466548.
- [8] Fangyu Li, Rui Xie, Zengyan Wang, Lulu Guo, Jin Ye, Ping Ma, Wenzhan Song, "Online Distributed IoT security Monitoring With Multidimensional Streaming Big data", *IEEE Internet of Things Journal*, Volume: 7, Issue: 5, Year: 2020
- [9] J. D. de Hoz Diego, J. Saldana, J. Fernández-Navajas and J. Ruiz-Mas, "Decoupling Security From Applications in CoAP-Based IoT Devices," in *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 467-476, Jan. 2020, doi: 10.1109/JIOT.2019.2951306.
- [10] W. Kang, J. Deng, P. Zhu, X. Liu, W. Zhao and Z. Hang, "Multi-dimensional Security Risk Assessment Model Based on Three Elements in the IoT System," *2020 IEEE/CIC International Conference on Communications in China (ICCC)*, Chongqing, China, 2020, pp. 518-523, doi: 10.1109/ICCC49849.2020.9238832.
- [11] A. S. Sheikh, A. Keerthi, S. Dhuli, G. Likhita, B. S. V. Naga Jahnavi and F. Atik, "A Novel Security System for IoT Applications," *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Kharagpur, India, 2021, pp. 1-5, doi: 10.1109/ICCCNT51525.2021.9579502.
- [12] B. Wei, G. Liao, W. Li and Z. Gong, "A Practical One-Time File Encryption Protocol for IoT Devices," *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, Guangzhou, China, 2017, pp. 114-119, doi: 10.1109/CSE-EUC.2017.206.
- [13] N. Kashyap, A. Rana, V. Kansal and H. Walia, "Enhanced Data Security and Authentication Techniques for IoT Devices on Cloud," *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India, 2021, pp. 1-6, doi: 10.1109/ICRITO51393.2021.9596232.
- [14] M. Asplund and S. Nadjm-Tehrani, "Attitudes and Perceptions of IoT Security in Critical Societal Services," *IEEE Access*, vol. 4, pp. 2130- 2138, 2016
- [15] Boheung Chung, Jeongyeo Kim, Youngsung Jeon, "On-demand security configuration for IoT devices", 2016 International Conference on Information and Communication Technology Convergence (ICTC), Year: 2016
- [16] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang and D. Chen, "Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach," in *IEEE Access*, vol. 7, pp. 9368-9383, 2019, doi: 10.1109/ACCESS.2018.2890432.

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization

Volume 12, Special Issue 1, April 2023

10th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '23)5th -6th April 2023

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

- [17] Caiming Liu, Yan Zhang, Zhonghua Li, Jiandong Zhang, Hongying Qin, Jinquan Zeng, "Dynamic Defense Architecture for the security of the Internet of Things", 2015 11th International Conference on Computational Intelligence and security (CIS), Year: 2015
- [18] S. Xiong, Q. Ni, L. Wang and Q. Wang, "SEM-ACSIT: Secure and Efficient Multiauthority Access Control for IoT Cloud Storage," in *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2914-2927, April 2020, doi: 10.1109/JIOT.2020.2963899.
- [19] Paul Loh Ruen Chze, Kan Siew Leong, "A secure multi-hop routing for IoT communication", 2014 IEEE World Forum on Internet of Things (WF-IoT), Year: 2014
- [20] K. R. Sollins, "IoT Big Data Security and Privacy Versus Innovation," in *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1628-1635, April 2019, doi: 10.1109/JIOT.2019.2898113
- [21] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the internet of things (IoT)," in Anonymous Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 420-429.
- [22] Y. Tao, P. Xu and H. Jin, "Secure Data Sharing and Search for Cloud-Edge-Collaborative Storage," in *IEEE Access*, vol. 8, pp. 15963-15972, 2020, doi: 10.1109/ACCESS.2019.2962600.
- [23] F. Alsubaei, A. Abuhusseini and S. Shiva, "Ontology-Based Security Recommendation for the Internet of Medical Things," in *IEEE Access*, vol. 7, pp. 48948-48960, 2019, doi: 10.1109/ACCESS.2019.2910087
- [24] I. -R. Chen, J. Guo, D. -C. Wang, J. J. P. Tsai, H. Al-Hamadi and I. You, "Trust-Based Service Management for Mobile Cloud IoT Systems," in *IEEE Transactions on Network and Service Management*, vol. 16, no. 1, pp. 246-263, March 2019, doi: 10.1109/TNSM.2018.2886379.
- [25] S. Siboni *et al.*, "Security Testbed for Internet-of-Things Devices," in *IEEE Transactions on Reliability*, vol. 68, no. 1, pp. 23-44, March 2019, doi: 10.1109/TR.2018.2864536.



SJIF: 8.423



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INTERNATIONAL CENTRE



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 **9940 572 462**  **6381 907 438**  **ijirset@gmail.com**



www.ijirset.com

Scan to save the contact details