International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-11 Issue-6, August 2022

ML Based Authentication Scheme for Data Storage in Cloud Based IoT

Bhushan B. Shaharkar, Darshan P. Pandit

Abstract: ***Today, organizations are using IoT devices to accurately collect real data and make better business decisions to increase customer satisfaction. The data collected should be stored and stored in a well-designed storage system, which encourages companies to review their data storage infrastructure. The company needs to store data created by the Internet of Things, and that data grows exponentially, forcing IoT to think about cloud storage for data storage. Security issues are a major concern when handling and processing data in DI and cloud environments. Secure integration of IoT and cloud computing, and introduced a model to ensure this integration. The secure database of any IoT operating system was suffers from poorly protected read and write functions, which limits data storage on any IoT platform. In addition, clouds can provide space to store a wide variety of data that plays an important role in the world of cyber security. However, large centralized systems operating in the cloud are also very vulnerable due to their power, so they can be transformed into a kind of double-edged sword. In this paper, we propose a novel secure lightweight authentication scheme for data storage (SLA-DS) in IoT and cloud server. The SLA-DS integrates IoT and cloud technology combination which mainly focuses on security issues.***

Keywords: ***Cloud Computing, Data Management, IoT, SLA-DS.***

I. INTRODUCTION

It is now common for smart objects to connect to the Internet, exchange data and information, and interact with users and other devices. These products are found in various fields such as health monitoring, telecommunications, automation, transportation, geriatrics and child care. [1][2]. This collection of associated substance is denominated Internet of things (IoT) [3]. IoT is not just a machine or network; it is an excellent and physical object that integrates technology for communication inside and outside the home. IoT defines an ecosystem that includes topics, communications, applications, data analysis, business opportunities, and innovation. [4]. IoT citizens can interact with codons, connect smart objects, interact in different contexts, use different protocols, and integrate the natural diversity of the environment [5]. Websites are created to explore and improve web solutions, such as the KNT meta-operating system, which focuses on integrating existing technology and software into IoT operating systems [6]. Nowadays, companies use IoT devices in real time and constantly collect data to make better business decisions to increase customer satisfaction. The company needs IoT data storage, and this data is growing significantly, making IoT think about storing data in cloud memory. IoT data storage cloud is an important choice as various companies value or understand this information [7][8]. Cloud memory has many advantages over storing IoT data on campus. Data management and storage management is a problem for the cloud provider, so use only computer services. The cloud is the best repository for storing and processing IoT data, but there are problems with using the cloud for IoT data storage. Cloud memory security is an important and vital issue [9][10]. Data collected from IoT devices are often very sensitive or very sensitive to organization. When using cloud memory, companies are concerned about cloud security issues. Many articles discuss complex issues such as secure packet sharing, short message authentication, IoT security issues, compromise attacks, layer attacks, and news content filtering [11][12]. In addition, IoT and cloud computing systems are considered independent units in most works. Integrated Data System - Unlocks the structure of an encrypted array journal for delayed updates and multiple data recovery [13]. IoT uses secure cloud storage services and bloom filters based on visual data retention [14]. The Data Integrity Check System is based on a short signature process (Z signature) that supports confidential trusted third party (TPA) confidentiality and public auditing [15]. During the signing process, the hash function is effectively reduced by reducing the invoice. Efficient and secure use of KNN request for data not stored on semi trusted cloud servers [16]. An enhanced policy-based puncturable encryption (P-PUN-ENC) [17] Cloud is the oldest and most secure data automation software in IoT. This allows data owners to strategically, accurately and permanently delete isolated IoT data without the need for a cloud server. CECS Secure Data Recovery and Sharing Software allows users to create and manage private and private key pairs Field servers are needed to manage users' private keys and to install community search keys to obtain secure, efficient and flexible data [18]. The CP-ABE based storage model is used for cloud storage for data storage and IoT applications. Cloud System Character Management Module (AAM) acts as an agent providing effective access control and significantly reduces the cost of public key collection overhead. [19].

Manuscript received on 30 July 2022 | Revised Manuscript received on 02 August 2022 | Manuscript Accepted on 15 August 2022 | Manuscript published on 30 August 2022.

***** Correspondence Author

Bhushan B. Shaharkar*, Department of Information Technology, Walchand Institute of Technology, Solapur (Maharashtra), India. Email: bbshaharkar@witsolapur.org

Darshan P. Pandit, Department of Computer Science and Engineering, Walchand Institute of Technology, Solapur (Maharashtra), India. Email: dppandit@witsolapur.org

DTLS evaluates protected copy controlled IoT devices and the three CAP security systems in the cloud and cloud related IoT systems [20].

II. LITERATURE SURVEY

Zhou et al. [21] have presented IoT based configuration validation program for cloud servers. It not only eliminates computational loading, but also creates software for resource-controlled objects such as sensors or IoT devices. Proper verification provided by Proverb ensures the security of a specific authorization program. Authentication program proves that it is protected from various attacks and simultaneously gains important security features such as user audit, cross-authentication and session security.

Alzubi et al. [22] IoT Schroder has developed the cost-effect in-tech Mac learning (HNS-CODML) system, which aims to quickly synchronize and enhance data sent through the cloud. First, the FSA network model represents the state and changes. The status here indicates the current state of the device and changes in device performance. During each session, the XORed function creates a basic layout using the hash tag Fair-shredder, which reduces the average running length and interacts with the individual parts of the output line. Finally, Cost Optimized Deep Secured (CODS) data is transmitted based on the expected and unpredictable value of the flag. Based on these two flags, it is said that there will be a secure transfer with low transmission costs and overhead costs.

Kavin et al. [23] have proposed a CRT-based protected storage program adopts fresh formula which introduces a second encryption program that uses the second encryption formula and the new cloud data encryption formula. Additionally, the team introduced a new formula with key generation functionality for retrieving encrypted data from the cloud on a cloud server. Evaluates the performance of security models through analysis of professional results. Finally, the data protection model is better than other existing models. Xu et al. [24] have presented an Attribute-based access control system for the IoT cloud introduces an effective attribute-based encryption program that allows the data owner to effectively manage data user certificates. Users can open the encryption key on a particular computer, and secret users can analyze the security of our program using appropriate resources and perform tests to show the high performance of a particular system. Xiong et al. [25] have proposed a key derivation encryption (KDE) algorithm is used to create a secure data deletion (SDDK) program for IoT devices. KDE algorithm for creating a node key tree, generating data keys, encrypting user-sensitive data, and managing keys based on the false fish memory array structure. SDDK program integrates cyber text, partial volume deletion, and key deletion after data extraction, and then securely deletes data on IoT devices. Thirumalai et al. [26] have proposed a the public key exponent secure scheme (ENPKESS) recommends the effective and comprehensive use of the non-linear deposit equation to provide further protection against lateral channel attacks such as time attacks. This program has three-phase encryption and two-phase encryption, and other programs such as ESR and RSA have encryption and encryption levels. For this reason, it is very difficult to establish the secret key of our society. Our algorithm is best suited for a secure cloud environment using the Internet of Things (IoT). We also used the NAP method to encrypt ENPKESS keys to ensure high security on cloud computers.

Sengupta et al. [27] have proposed a Cloud Toilet Assist Integrated e-Health Architecture aims to access live data using this e-Health Architecture cloud via IoT. Within this framework, implement a health data management plan to store large amounts of health data and meet the health data needs of the end user. They used the NoSQL based model to store health data. The performance of a particular model is calculated based on data transfer time, power consumption, request response time, and data packet loss. Finally, the evaluation results of our particular model are comparable to the performance of a cloud-based e-health system, justifying the fact that our specific model applies to cloud-based e-health solutions. Wang et al. [28] have proposed A secure health monitoring framework that integrates NDN-based IOT and cloud computing. The NDN program uses this framework to improve the efficiency of medical data recovery, and uses cyber text and signatures to ensure the security of medical data transmission. The performance of the frames is evaluated. Delays and costs in obtaining medical data were reduced by 28% and 52%, respectively. The security features of the proposed program are similar to the current method, as the proposed program uses a medical encryption method, such as the Advanced Encryption Standard, to safely distribute medical programs.

III. METHODOLOGY

Machine learning (ML) techniques severely rely on the data. Once data is gathered, it is integrated for training, validation and test datasets. The dataset used in creating the ML model is often represented as training data and labels which are related with training data if the user is alert of the data description. Here we analyze different machine learning technique for improving both data aggregation in IoT and data storage in cloud server. Where ML act as a fundamental component of IoT and cloud platform. Machine learning is used to provides fast results with device connectivity and management. It also helpful for application enablement and integration, streaming analytics, and a model for deployment. It also expands the supports for the cloud, on-premises and/or at the edge. Machine Learning is intended to help us to develop new machine learning models through existing ML model. AutoML provides precise machine learning model to be selected based on our data, whether that can be past data warehoused in big data records or working device data captured on the IoT platform. Tensorflow, Keras, Scikit-learn used for developing machine learning models. IoT Machine Learning permits the models to be developed in different framework of data science domain. These models can be transformed into industry-standard formats using FOSS in IoT.

It also provides accelerated training and inference for large amount of data. IoT-ML is imported from different framework of data science frameworks or the data generated by IoT device itself, these models are deployed directly on to the cloud platform or at edge device single click. The working models can be easily managed and monitored for data aggregation. It also allows quick updating based on generated data patterns. These tested and verified models are immediately made available for deployment in cloud-IoT platform.Multi-Dimensional Access Control (MD-AC) can be used in a clean environment to maintain the privacy of IoT services. This software helps in dynamic authentication and cloud computing for many officers. Test results indicate that MD-AC can assess access requirements during reasonable and acceptable processing. Due to the more complex test conditions and larger transactions, the average encryption and encryption time are 18 and 10, respectively. In addition, specific projects were studied and compared with recent complex projects. The results show that a particular program is fast and powerful against various known attacks [29].

lightweight secure audit cloud memory with data dynamics supports multiple update functions that improve security feature. Data Dynamics algorithm offers approval time and a second source time which provides new statistics on deep memory that can be easily verified through a public audit [30].

The lightweight authentication mechanism for securing cloud-based IoT environment (LAM-CIoT) to address security issues needed for it. Rigorous LAM-CIoT security analysis using the ROR model, systematic security testing using the AVISPA tool, and informal security suggest that LAM-CIoT can withstand many well-known attacks. LAMCIoT supports the addition of a new IoT sensor to the network after the initial installation, as well as the password setting and the biometric update phase. An unclear extraction mechanism is also used at the end of the user for local biometric verification. LAMCIoT is systematically analyzed for its safety zone and adequately protected using a widely accepted "true or random" model [31]. Here we propose a secure lightweight authentication scheme for data storage (SLA-DS) to improve security issue, resulting from integration. Initially hybrid sign encryption-based KDE algorithm is used to generate data key for each user, which enhances the key management process. It also provide data encryption and decryption technique for secure transmission of messages from IoT nodes to cloud server and vice-versa.

To make use of novel lightweight authentication scheme i.e. N-SUPREME which identifies correctness of data arriving from correct node.

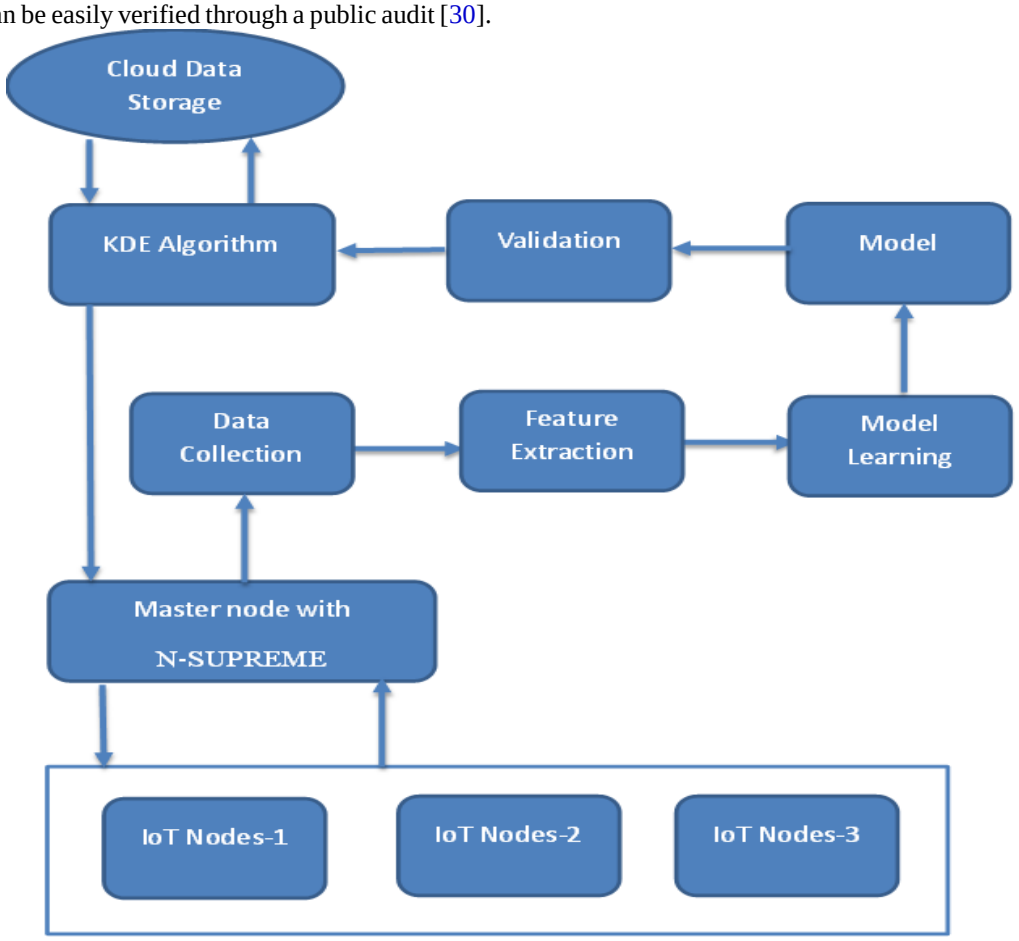

Figure-1: Secure lightweight authentication scheme for data storage (SLA-DS)

Figure-1 depicts the fundamental structure of Secure lightweight authentication scheme for data storage where IoT nodes generate data, these data collected and managed by N-SUPREME master node. The main function of master node is to monitored the data retrieving from the authorized IoT nodes or devices which are computed locally. After authorization appropriate all data is collected at data collection module. The feature extraction will be carried out on collected data where raw data is transformed to numerical attribute.

These attributes are utilized for data processing which generates meaningful information. This information is again used for model learning where we use training sequence of the data. Based on the training sequence a model is generated which is tested in the validation phase. After completion of validation phase, a secure key generation technique KDE algorithm is used to transfer the data to the cloud storage in an encrypted form. The data is again retrieved back by decryption the information through KDE algorithm and sending back to sensor nodes through master node device.

IV. CONCLUSION

Cloud-IoT connects a huge number of nodes and edge node which will lead to a huge amount of data to be monitored and managed. In this paper, we proposed a novel secure lightweight authentication scheme for data storage (SLA-DS) in IoT and cloud server. The SLA-DS integrates IoT and cloud technology combination which mainly focuses on security issues. This scheme can be evaluated using both NS2 and Net beans for the IoT network data gathering, aggregation performance analysis and cloud storage performance analysis respectively. This scheme ensures that only valid users can access data and the services provided by the cloud platform that engages in attribute-based encryption technique to preserving data integrity and privacy of the network. The communication messages between the server and node travel through secure channel in an encrypted format which enables for the user to keep his information secure. Here data encryption and decryption overhead have been increased by this scheme but this can be reduced further in future by advanced lightweight deep neural network (Q-DNN) scheme

REFERENCES

1. Hwang, J., Aziz, A., Sung, N., Ahmad, A., Le Gall, F. and Song, J., 2020. AUTOCON-IoT: Automated and Scalable Online Conformance Testing for IoT Applications. IEEE Access, 8, pp.43111-43121. [CrossRef]
2. Vamseekrishna, A., Madhav, B.T.P., Anilkumar, T. and Reddy, L.S.S., 2019. An IoT Controlled Octahedron Frequency Reconfigurable Multiband Antenna for Microwave Sensing Applications. IEEE Sensors Letters, 3(10), pp.1-4. [CrossRef]
3. Samaila, M.G., Sequeiros, J.B., Simões, T., Freire, M.M. and Inácio, P.R., 2020. IoT-HarPSecA: A Framework and Roadmap for Secure Design and Development of Devices and Applications in the IoT Space. IEEE Access, 8, pp.16462-16494. [CrossRef]
4. Lazarescu, M.T., 2013. Design of a WSN platform for long-term environmental monitoring for IoT applications. IEEE Journal on emerging and selected topics in circuits and systems, 3(1), pp.45-54. [CrossRef]
5. Roy, D.S., Behera, R.K., Reddy, K.H.K. and Buyya, R., 2018. A context-aware fog enabled scheme for real-time cross-vertical IoT applications. IEEE Internet of Things Journal, 6(2), pp.2400-2412. [CrossRef]
6. Rafique, W., Zhao, X., Yu, S., Yaqoob, I., Imran, M. and Dou, W., 2020. An Application Development Framework for Internet-of-Things Service Orchestration. IEEE Internet of Things Journal, 7(5), pp.4543-4556. [CrossRef]
7. Zhu, H., Yuan, Y., Chen, Y., Zha, Y., Xi, W., Jia, B. and Xin, Y., 2019. A secure and efficient data integrity verification scheme for cloud-IoT based on short signature. IEEE Access, 7, pp.90036-90044. [CrossRef]
8. Hao, J., Liu, J., Wu, W., Tang, F. and Xian, M., 2019. Secure and Fine-Grained Self-Controlled Outsourced Data Deletion in Cloud-Based IoT. IEEE Internet of Things Journal, 7(2), pp.1140-1153. [CrossRef]
9. Hur, J., Koo, D., Shin, Y. and Kang, K., 2016. Secure data deduplication with dynamic ownership management in cloud storage. IEEE Transactions on Knowledge and Data Engineering, 28(11), pp.3113-3125. [CrossRef]
10. Sharma, P.K., Chen, M.Y. and Park, J.H., 2017. A software defined fog node based distributed blockchain cloud architecture for IoT. Ieee Access, 6, pp.115-124. [CrossRef]
11. Dehury, C.K. and Sahoo, P.K., 2016. Design and implementation of a novel service management framework for IoT devices in cloud. Journal of Systems and Software, 119, pp.149-161. [CrossRef]
12. Celesti, A., Fazio, M., Villari, M. and Puliafito, A., 2016. Adding long-term availability, obfuscation, and encryption to multi-cloud storage systems. Journal of Network and Computer Applications, 59, pp.208-218. [CrossRef]
13. He, J., Zhang, Z., Li, M., Zhu, L. and Hu, J., 2018. Provable data integrity of cloud storage service with enhanced security in the internet of things. IEEE Access, 7, pp.6226-6239. [CrossRef]
14. Jeong, J., Joo, J.W.J., Lee, Y. and Son, Y., 2019. Secure cloud storage service using bloom filters for the internet of things. IEEE Access, 7, pp.60897-60907. [CrossRef]
15. Zhu, H., Yuan, Y., Chen, Y., Zha, Y., Xi, W., Jia, B. and Xin, Y., 2019. A secure and efficient data integrity verification scheme for cloud-IoT based on short signature. IEEE Access, 7, pp.90036-90044. [CrossRef]
16. Guo, C., Zhuang, R., Su, C., Liu, C.Z. and Choo, K.K.R., 2019. Secure and Efficient ${K} $ Nearest Neighbor Query Over Encrypted Uncertain Data in Cloud-IoT Ecosystem. IEEE Internet of Things Journal, 6(6), pp.9868-9879. [CrossRef]
17. Hao, J., Liu, J., Wu, W., Tang, F. and Xian, M., 2019. Secure and Fine-Grained Self-Controlled Outsourced Data Deletion in Cloud-Based IoT. IEEE Internet of Things Journal, 7(2), pp.1140-1153. [CrossRef]
18. Tao, Y., Xu, P. and Jin, H., 2019. Secure Data Sharing and Search for Cloud-Edge-Collaborative Storage. IEEE Access, 8, pp.15963-15972. [CrossRef]
19. Xiong, S., Ni, Q., Wang, L. and Wang, Q., 2020. SEM-ACSIT: Secure and Efficient Multiauthority Access Control for IoT Cloud Storage. IEEE Internet of Things Journal, 7(4), pp.2914-2927. [CrossRef]
20. Raza, S., Helgason, T., Papadimitratos, P. and Voigt, T., 2017. SecureSense: End-to-end secure communication architecture for the cloud-connected Internet of Things. Future Generation Computer Systems, 77, pp.40-51. [CrossRef]
21. Zhou, L., Li, X., Yeh, K.H., Su, C. and Chiu, W., 2019. Lightweight IoT-based authentication scheme in cloud computing circumstance. Future Generation Computer Systems, 91, pp.244-251. [CrossRef]
22. Xu, S., Yang, G., Mu, Y. and Liu, X., 2019. A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance. Future Generation Computer Systems, 97, pp.284-294. [CrossRef]
23. Ganapathy, S., 2019. A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications. Computer Networks, 151, pp.181-190. [CrossRef]
24. Alzubi, J.A., Manikandan, R., Alzubi, O.A., Qiqieh, I., Rahim, R., Gupta, D. and Khanna, A., 2020. Hashed Needham Schroeder Industrial IoT based Cost Optimized Deep Secured data transmission in cloud. Measurement, 150, p.107077. [CrossRef]
25. Sengupta, S. and Bhunia, S.S., 2020. Secure Data Management in Cloudlet assisted IoT Enabled e-Health Framework in Smart City. IEEE Sensors Journal. [CrossRef]
26. Xiong, J., Chen, L., Bhuiyan, M.Z.A., Cao, C., Wang, M., Luo, E. and Liu, X., 2020. A secure data deletion scheme for IoT devices through key derivation encryption and data analysis. Future Generation Computer Systems, 111, pp.741-753. [CrossRef]
27. Thirumalai, C., Mohan, S. and Srivastava, G., 2020. An efficient public key secure scheme for cloud and IoT security. Computer Communications, 150, pp.634-643. [CrossRef]
28. Wang, X. and Cai, S., 2020. Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud. Future Generation Computer Systems. [CrossRef]
29. Riad, K., Huang, T. and Ke, L., 2020. A dynamic and hierarchical access control for IoT in multi-authority cloud storage. Journal of Network and Computer Applications, p.102633. [CrossRef]
30. Li, L. and Liu, J., 2020. SecACS: Enabling lightweight secure auditable cloud storage with data dynamics. Journal of Information Security and Applications, 54, p.102545. [CrossRef]
31. Wazid, M., Das, A.K., Bhat, V. and Vasilakos, A.V., 2020. LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. Journal of Network and Computer Applications, 150, p.102496 [CrossRef]

AUTHORS PROFILE

Mr. Bhushan B. Shahaharkar, working as an Assistant Professor at Dept of Information Technology, Walchand Institute of Technology, Solapur, MH. and pursuing the Ph.D in Computer Science and Engineering in K.L University, Vijayawada, Andhra Pradesh, India. He is expertise in cloud-computing, computer networks and distributed systems.

Mr. Darshan Pradeep Pandit, working as an Assistant Professor at Dept of Computer Science and Engineering, Walchand Institute of Technology, Solapur, MH. and pursuing the Ph. D in Computer Science and Engineering in K.L University, Vijayawada, Andhra Pradesh, India. He is expertise in Internet of Things, computer graphics and software engineering.