Efficient Encryption Protocol

Ms. J. Dhanalakshmi[1], Mr. L. Sriram Prasath[2], Mr. S. Sridharan[3], Mr .J .Jeeva[4], Mr .S. Sriram[5]
[1]Assistant professor, Dept of Computer Science and Engineering
[2, 3, 4, 5]Dept of Computer Science and Engineering
[1, 2, 3, 4, 5] SSM Institute of Engineering and Technology, Dindigul

Abstract- *Industrial Internet of Things (IoT) has suffered from insufficient identity authentication and dynamic network topology, thereby resulting in vulnerabilities to data confidentiality. Recently, the attribute based encryption (ABE) schemes have been regarded as a solution to ensure data transmission security and the fine-grained sharing of encrypted IoT data. However, most of existing ABE schemes that bring tremendous computational cost is not suitable for resources-constraint IoT devices.Therefore, lightweight and efficient data sharing and searching schemes suitable for IoT applications are of great importance. To this end, we propose a light searchable attribute based encryption scheme (namely LSABE). Our scheme can significantly reduce the computing cost of IoT devices with the provision of multiple*

Keywords- Searching for data users. Meanwhile, we extend the LSABE scheme to multi-authority scenarios so as to effectively generate and manage the public/secret keys in the distributed IoT environment. Finally, the experimental results demonstrate thatOur schemes can significantly maintain computational efficiency and save the computational cost at IoT devices, compared to other existing schemes.

I. INTRODUCTION

Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software. Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it. Cloud computing is a popular option for people and businesses for a number of reasons including cost savings, increased productivity, speed and efficiency, performance, and security. Cloud computing is named as such because the information being accessed is found remotely in the cloud or a virtual space. Companies that provide cloud services enable users to store files and applications on remote servers and then access all the data via the Internet. This means the user is not required to be in a specific place to gain access to it, allowing the user to workremotely.Cloud computing takes all the heavy lifting involved in crunching and processing data away from the device you carry around or sit and work at. It also moves all of that work to huge computer clusters far away in cyberspace. The Internet becomes the cloud and voilà your data, work, and applications are available from any device with which you can connect to the Internet, anywhere in the world.Cloud computing can be both public and private. Public cloud services provide their services over the Internet for a fee. Private cloud services, on the other hand, only provide services to a certain number of people. These services are a system of networks that supply hosted services. There is also a hybrid option, which combines elements of both the public and private services.

II. PROPOSEDSYSTEM

A Lightweight Searchable Attribute Based Encryption is the LSABE-MA. LSABE-MA functions for the multi-authority, which necessitates collaboration between a number of authorities to provide the user's key. The majority of other methods use single authorities, which may cause the private key to be revealed. Additionally, compared to previous single-authority systems, our LSABE plan offers lower computational expenses. Data encryption in LSABE-MA is carried out by sensor nodes with a limited amount of resources. Immediately upload encrypted privacy-sensitive content to the cloud from the actual IoT environment. As a result, the encryption process depends greatly on delay. Our LSABE-MA keyword search algorithm needs keys and generating operations. When compared to other systems, this overhead is not very large. In actuality, the cloud server does the search such that for cloud servers with powerful computational capabilities, this overhead can be minimal. We present this method in order to address the security issues that the current system has and efficiently store data on the cloud. Tens of thousands of mining nodes in the network digitally sign and confirm each transaction in the ledger.

III. RELATED WORK

In 2020, F. Farivar, M. S. Haghighi, A. Jolfaei, and M. Alazab were proposed a hybrid intelligent-classic control approach for reconstruction and compensation of cyber-attacks launched on inputs of nonlinear cyber-physical systems (CPS) and industrial Internet of Things systems, which work through shared communication networks. In this article, a class of n-order nonlinear systems is considered as a

model of CPS while it is in presence of cyber-attacks only in the forward channel. An intelligent-classic control system is developed to compensate cyber-attacks. Neural network (NN) is designed as an intelligent estimator for attack estimation and a classic nonlinear control system based on the variable structure control method is designed to compensate the effect of attacks and control the system performance in tracking applications. In the proposed strategy, nonlinear control theory is applied to guarantee the stability of the system when attacks happen. In this strategy, a Gaussian radial basis function NN is used for online estimation and reconstruction of cyber-attacks launched on the networked system.

In 2020, S. Ghane, A. Jolfaei, L. Kulik, K. Ramamohanarao, and D. Puthal were proposed an article based on IOT Technologies.In this paper,Vehicles are advancing from stand-alone transportation means to vehicle-to-vehicle, and vehicle to infrastructure communications enabled devices which are able to exchange data through the transportation communication infrastructure. As the IoT and data remain intrinsically linked together, the fast-changing mobility landscape of intent-based networking for the Internet of connected vehicles comes with a great risk of data security and privacy violations. This paper considers the privacy issues in the distributed edge computing, in which the data is communicated between a number of vehicles in the IoT layer and potentially untrusted edge controllers at the edge of the network. The sensory data communicated by the vehicles contain sensitive information, such as location and speed, which could violate the users' privacy if they are leaked with no perturbation. Recent studies suggest mechanisms for randomizing the stream of data to ensure individuals' privacy. Although the past works on differential privacy provide a strong privacy guarantee, they are limited to applications where communication parties are trusted and/or there is no correlation between the users or the featured of sensory data.

In 2020,J. Sun, H. Xiong, X. Liu, Y. Zhang, X. Nie, and R. H. Deng. The booming of Internet of Things (IoT), smart health (s-health) is becoming an emerging and attractive paradigm. It can provide accurate prediction of various diseases, improve the quality of healthcare. Nevertheless, data security and user privacy concerns still remain as issues to be addressed. As a highly potential and prospective solution to secure IoT-oriented s-health applications, Ciphertext policy attribute based encryption (CP-ABE) schemes raise challenges such as heavy overhead and attribute privacy of the end users. To resolve these drawbacks, an optimized vector transformation approach is first proposed to efficiently transform the access policy and user attribute set into respective vectors of shorter length while other approaches result in redundant and longer vectors. Our transformation approach can greatly relieve the costly overheard of key generation, encryption and decryption phases. Then, based on the transformation approach and the offline/online computation technology, we propose a lightweight policy-hiding CP-ABE scheme for the IoT-oriented s-health application. With our proposed scheme, data users in s-health system can perform lightweight encryption and decryption without leaking any sensitive privacy about attributes of the user.

In 2019, M. Usman, M. A. Jan, X. He, and J. Chen were proposed a concept of Internet of Multimedia Things (IoMT) is becoming popular nowadays and can be used in various smart city applications, e.g., traffic management, healthcare, and surveillance. In the IoMT, the devices, e.g., Multimedia Sensor Nodes (MSNs), are capable of generating both multimedia and non-multimedia data. The generated data are forwarded to a cloud server via a Base Station (BS). However, it is possible that the Internet connection between the BS and the cloud server may be temporarily down. The limited computational resources restrict the MSNs from holding the captured data for a longer time. In this situation, mobile sinks can be utilized to collect data from MSNs and upload to the cloud server. However, this data collection may create privacy issues, such as revealing identities and location information of MSNs. Therefore, there is a need to preserve the privacy of MSNs during mobile data collection. In this paper, we propose an efficient privacy-preserving-based data collection and analysis (P2DCA) framework for IoMT applications. The proposed framework partitions an underlying wireless multimedia sensor network into multiple clusters. Each cluster is represented by a Cluster Head (CH).

In 2019,A. Jolfaei and K. Kant. Considers data security and privacy issues in intelligent transportation systems which involve data streams coming out from individual vehicles to road side units. In this environment, there are issues in regards to the scalability of key management and computation limitations at the edge of the network. To address these issues, we suggest the formation of groups in the vehicular layer, where a group leader is assigned to communicate with group members and the road side unit. We propose a lightweight permutation mechanism for preserving the confidentiality and privacy of sensory data.

In 2019,S. Tan, K. Yeow, and S. O. Hwang.The enhancement of a lightweight key-policy attribute-based encryption (KP-ABE) scheme designed for the Internet of Things (IoT). The KP-ABE scheme was claimed to achieve Ciphertext in distinguishability under chosen-plaintext attack in the selective-set model but we show that the KP-ABE scheme is insecure even in the weaker security notion, namely,

one-way encryption under the same attack and model. In particular, we show that an attacker can decrypt a Ciphertext which does not satisfy the policy imposed on his decryption key. Subsequently, we propose an efficient fix to the KP-ABE scheme as well as extending it to be a hierarchical KP-ABE (H-KP-ABE) scheme that can support role delegation in IoT applications. An example of applying our H-KP-ABE on an IoT-connected healthcare system is given to highlight the benefit of the delegation feature. Lastly, using the NIST curves secp192k1 and secp256k1, we benchmark the fixed (hierarchical) KP-ABE scheme on an Android phone and the result shows that the scheme is still the fastest in the literature.
In 2018,Y. Yang, X. Liu, X. Zheng, C. Rong, and W. Guo.In this article, Secure search over encrypted remote data is crucial in cloud computing to guarantee the data privacy and usability. To prevent unauthorized data usage, fine-grained access control is necessary in multi-user system. However, authorized user may intentionally leak the secret key for financial benefit. Thus, tracing and revoking the malicious user who abuses secret key needs to be solved imminently. In this paper, we propose an escrow free traceable attribute based multiple keywords subset search system with verifiable outsourced decryption (EF-TAMKS-VOD). The key escrow free mechanism could effectively prevent the key generation centre (KGC) from unscrupulously searching and decrypting all encrypted files of users. Also, the decryption process only requires ultra-lightweight computation, which is a desirable feature for energy-limited devices. In addition, efficient user revocation is enabled after the malicious user is figured out. Moreover, the proposed system is able to support flexible number of attributes rather than polynomial bounded.Flexible multiple keyword subset search pattern is realized, and the change of the query keywords order does not affect the search result. Security analysis indicates that EF-TAMKS-VOD is provably secure.

IV. MODULES

MODULE DESCRIPTION

- Data Owner
- Attribute Authority
- File Choose
- Encryption
- Cloud Server
- Auxiliary Cloud Server
- Data User
- Certificate Authority
- Decryption

DATA OWNER-

- The data owner who entered into the cloud should be registered.
- In registration process user has to input their details like user name, email address, gender, name and the password they want to access.
- The data owner given the keyword to store in cloud server.

ATTRIBUTE AUTHORITY-

- The attribute authority to generating a public key and secret key and storing to the cloud server.
- The secret keys are using encryption and decryption process then storing the cloud server.

FILE CHOOSE-

- This process going to select our data set and then to uploaded.
- Health dataset to using our projects.
- After this process to view our dataset.
- To check our whole data set correct or wrong.

ENCRYPTION-

- The data is encrypted for secure maintenance. So that the unauthorized person cannot be able to access the data that are presented in the cloud server and auxiliary server.
- Each file contains health record, this process to using algorithm for LSABE.
- In this process to using secret key for the encryption process then storing cloud server and auxiliary cloud server.

CLOUD SERVER-

- After that completed encrypted process to be stored in the cloud storages.
- The any one to not open the encrypted files.
- The data user searching for the trapdoor keys.
- It’s securable for our encrypted data’s.
- Computing services will be able to encrypt documents to keep them safe in the cloud server.

AUXILIARY CLOUD SERVER-

- The auxiliary cloud server is same process for cloud server.
- One of the storage purposes for this cloud server.

- This process to receiving the request for data users and then to sending the acknowledgement.

DATA USER-

- The data user going to register our details username, password, gender, email id, name.
- The certificate authorities access your id then login to your account.
- The user searching for trapdoor key in cloud server.
- Then sending to the transformation key for auxiliary cloud server.
- Sending decryption key and acknowledgement for auxiliary cloud server.

To decryption process complete to view our particular files

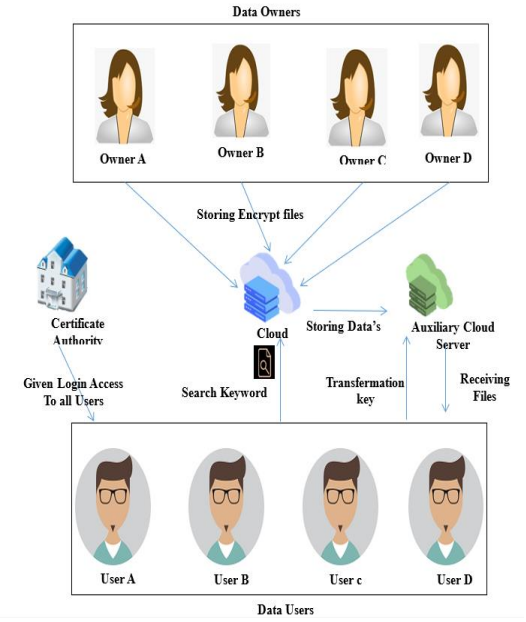
CERTIFICATE AUTHORITY-

- The data user register our details in register form and then to view the our details.
- If the any irrelevant user to reject our login access.
- The certificate authority to given permission to enter your account, otherwise you will not enter your account.

DECRYPTION-

- To select the particular encrypted file and then to using the secret key then decrypting the files.
- The LSABE means Lightweight Searchable Attribute Based Encryption and Secret key using our project.
- Completed the decrypt process then to storing the decrypted file in cloud server and auxiliary cloud server.
- In this process to one by one running our decrypting process in particular Data user account.

V. SYSTEM ARCHITECTURE



VI. CONCLUSION

LSABE scheme, which can support multi keyword search, fine grained access control and lightweight decryption. We also define the security notions of LSABE and prove that our schemes can secure against the chosen-keyword attack and the chosen-plaintext attack. Furthermore, we propose an improved version of LSABE, namely LSABE-MA to support the multi-authority scenario. LSABE-MA is more applicable to industrial IoT environment. The functional analysis shows that both LSABE and LSABEMA schemes require less storage and computing cost than most of the existing schemes. Experimental results on a real industrial system also demonstrate that our LSABE and LSABEMASchemes outperform other representative schemes. The feasibility analysis in IoT devices proves that our LSABE and LSABE-MA schemes can be well adapted in industrial IoT environment.

VII. FUTURE ENHANCEMENT-

The Future work, LSABE scheme supports stronger attribute privacy protection, lightweight and fine grained access policy, online encryption and efficient decryption

REFERENCES

[1] M. Usman, A. Jolfaei, and M. A. Jan, "RaSEC: An Intelligent Framework for Reliable and Secure Multi-Level Edge Computing in Industrial Environments," IEEE Trans. on Industry Applications, pp. 1–1, 2020.
[2] F. Farivar, M. S. Haghighi, A. Jolfaei, and M. Alazab, "Artificial Intelligence for Detection, Estimation, and

Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT," IEEE Trans. on Industrial Informatics, vol. 16, no. 4, pp. 2716–2725, 2020.

[3] S. Ghane, A. Jolfaei, L. Kulik, K. Ramamohanarao, and D. Puthal, "Preserving privacy in the internet of connected vehicles," IEEE Trans. on Intelligent Transportation Systems, pp. 1–10, 2020.

[4] M. Usman, M. A. Jan, X. He, and J. Chen, "P2DCA: A Privacy- Preserving-Based Data Collection and Analysis Framework for IoMT Applications," IEEE JSAC, vol. 37, no. 6, pp. 1222–1230, June 2019.

[5] A. Jolfaei and K. Kant, "Privacy and security of connected vehicles in intelligent transportation system," in 2019 DSN, June 2019, pp. 9–10.

[6] M. Green, S. Hohenberger, B. Waters et al., "Outsourcing the decryption of ABE ciphertexts," in USENIX Security, vol. 2011, no. 3, 2011.

[7] Y. Yang, X. Liu, X. Zheng, C. Rong, and W. Guo, "Efficient Traceable Authorization Search System for Secure Cloud Storage," IEEE Trans. on Cloud Computing, pp. 1–1, 2018.

[8] S. Tan, K. Yeow, and S. O. Hwang, "Enhancement of a lightweightattribute-based encryption scheme for the internet of things," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6384–6395, 2019.

[9] J. Sun, H. Xiong, X. Liu, Y. Zhang, X. Nie, and R. H. Deng, "Lightweight and Privacy-Aware Fine-Grained Access Control for IoToriented Smart Health," IEEE Internet of Things Journal, pp. 1–1, 2020.

[10] Y. Miao, J. Ma, X. Liu, X. Li, Z. Liu, and H. Li, "Practical attributebased multi-keyword search scheme in mobile crowdsourcing," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 3008–3018, Aug 2018.

[11] Y. Miao, X. Liu, R. H. Deng, H. Wu, H. Li, J. Li, and D. Wu, "Hybrid Keyword-Field Search with Efficient Key Management for Industrial Internet of Things," IEEE Trans. on Industrial Informatics, pp. 1–1, 2018.

[12] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing," IEEE Trans. on Services Computing, vol. 10, no. 5, pp. 785–796, Sep. 2017.

[13] J. Wei, W. Liu, and X. Hu, "Secure and efficient attribute-based access control for multiauthority cloud storage," IEEE Systems Journal, vol. 12, no. 2, pp. 1731–1742, 2018.

[14] K. Sowjanya, M. Dasgupta, S. Ray, and M. S. Obaidat, "An efficient elliptic curve cryptography-based without pairing kpabe for internet of things," IEEE Systems Journal, vol. 14, no. 2, pp. 2154–2163, 2020.

[15] J. Cui, H. Zhou, H. Zhong, and Y. Xu, "AKSER: Attribute-based keyword search with efficient revocation in cloud computing," Information Sciences, vol. 423, pp. 343–352, Jan. 2018.

[16] R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment," Future Generation Computer Systems, vol. 78, pp. 1005–1019, 2018.

[17] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in 2007 IEEE Symposium on Security and Privacy (SP '07). Berkeley, CA: IEEE, May 2007, pp. 321–334.

[18] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the internet of things," Future Generation Computer Systems, vol. 49, pp. 104–112, 2015.

[19] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public Key Encryption with Keyword Search," in Advances in Cryptology - EUROCRYPT, 2004, pp. 506–522.

[20] J. Li and L. Zhang, "Attribute-based keyword search and data access control in cloud," in 2014 Tenth International Conference on Computational Intelligence and Security. IEEE, 2014, pp. 382–386.