A NEW IMPLEMENTATION OF ADVANCED SECRED DATA SHARING SCHEME FOR IN CLOUD-ASSISTED IOT

Ms.C.Monisha, M.E – II[nd] year, CSE, P.S.V. College of Engineering & Technology, Krishnagiri.
Prof.C.Prakash Narayanan, Assistant Professor, Department of Computer Science and Engineering, P.S.V. College Of Engineering & Technology, Krishnagiri.

ABSTRACT

The explosive proliferation of Internet of Things (IoT) devices is generating an incomprehensible amount of data. Machine learning plays an imperative role in aggregating this data and extracting valuable information for improving operational and decision-making processes. In particular, emerging machine intelligence platforms that host pre-trained machine learning models are opening up new opportunities for IoT industries. While those platforms facilitate customers to analyze IoT data and de-liver faster and accurate insights, end users and machine learning service providers (MLSPs) have raised concerns regarding security and privacy of IoT data as well as the pre- trained machine learning models for certain applications such as healthcare, smart energy, etc. In this paper, we propose a cloud-assisted, privacy-preserving machine learning classification scheme over encrypted data for IoT devices. Our scheme is based on a three-party model coupled with a two-stage decryption Paillier-based crypto system, which allows a cloud server to interact with MLSPs on behalf of the resource- constrained IoT devices in a privacy-preserving manner, and shift load of computation- intensive classification operations from them. The detailed security analysis and the extensive simulations with different key lengths and number of features and classes demonstrate that our scheme can effectively reduce the overhead for IoT devices in machine learning classification applications. This project is developed by using Dotnet As front end and Sql server as back end.

1. INTRODUCTION

The Internet of things (IoT) industry is considered a most promising industry in the future. As forecast by Cisco and Ericsson, more than 20 billion of IoT devices will be connected to the Internet by 2021 [1]. The IoT platform connects a huge number of sensors to the data network to collect realtime data that was previously unavailable or at a scale that was previously unreachable. More importantly, it integrates the ubiquitous sensing capability with advanced computing and data analysis capabilities of backend

applications to provide automated extraction of insights by making sense of plethora of data generated by these sensors. This has led to a pervasive deployment of intelligence into our daily life, ranging from healthcare (e.g., remote patient monitoring, wearable fitness tracking) and security (e.g., community monitoring) to home automation, smart communities and smart cities (e.g., smart traffic control, distributed pollution monitoring).

In the IoT platform, the frontend IoT devices are usually resource- constrained, which have very limited storage and computing power to support complicated computations. Therefore, the intelligence is often provided by machine learning applications running on powerful backend servers. With the large volume of data generated by IoT devices, these servers map feature vectors to categorical or real-valued outputs to train predictive models, which output classification or predication results for future sensing data to the clients. For example, wearable devices with accelerometer and gyroscope, depth cameras, etc. are deployed in the home of old adults for fall detection. With real-time sensor data, the predictive model running on the server analyzes the vertical tate of objects and notify the caregiver when a fall is detected. More automatic medical assessment and risk profiling services can be provided from analyzing the physical measurements collected by the clients' wearable fitness tracking devices. The success of machine learning (ML) on IoT platforms has led to an explosion of demands. In fact, providing classification and predication services that are customized to different application domains is becoming an emerging business paradigm, known as "machine-learning-as-a-service" (MLaaS). Major cloud service providers such as Amazon, Google, Microsoft, and BigML are offering cloud-based MLaaS, which trains predictive models and charges future usage of the model at a pay-per-query orsubscription-based cost.

2. LITERATURE SURVEY

1) Privacy-preserving query over encrypted graph-structured data in cloudComputing

AUTHORS: N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou,

In the emerging cloud computing paradigm, data owners become increasingly motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. For the consideration of users' privacy, sensitive data have to be encrypted before outsourcing, which makes effective data utilization a very challenging task. In this paper, for the first time, we define and solve the problem of privacy-preserving query over encrypted graph-structured data in

cloud computing (PPGQ), and establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. Our work utilizes the principle of "filtering-and- verification". We prebuild a feature-based index to provide feature-related information about each encrypted data graph, and then choose the efficient inner product as the pruning tool to carry out the filtering procedure. To meet the challenge of supporting graph query without privacy breaches, we propose a secure inner product computation technique, and then improve it to achieve various privacy requirements under the known-background threat model.

2) Securing mhealthcare social networks: challenges, countermeasures andfuture directions

AUTHORS: J. Zhou, Z. Cao, X. Dong, X. Lin, and A. V. Vasilakos

M-healthcare mobile social network has emerged as a promising next-generation healthcare system increasingly adopted by the US and European governments, with the rapid development of sensor and wireless communication technologies. In this paper, we describe the goals and tactics, and present a distributed architecture of m- healthcare social networks. Following each kind of security and privacy challenge, we define a series of basic and sophisticated cyber attacks and give substantial and promising solutions to satisfy the unique security and privacy requirements in m- healthcare social networks. Last but not least, several interesting open problems are pointed out with possible addressing ideas to trigger more research efforts in this emerging area

3) Attribute-based encryption for fine-grained access control of encrypteddata

AUTHORS: V. Goyal, O. Pandey, A. Sahai, and B. WatersAs more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt.

4) Efficient remote user authentication scheme using smart card

AUTHORS: R. Lu and Z. CaoIn this paper, we propose a new remote user authentication scheme using smart card. In our scheme, there are two attractive features: (i) no verification tables are required in the remote server; (ii) only one hash function computation and one modular multiplication computation are costed in smart card. Therefore, compared with other schemes, our scheme is more efficient.

5) Secure e-health architecture based on the appliance of pseudonymization AUTHORS: B. Riedl, V. Grascher, and T. Neubauer

Due to the cost pressure on the health care system an increase in the need for electronic healthcare records (EHR) could be observed in the last decade, because EHRs promise massive savings by digitizing and centrally providing medical data. As highly sensitive patient information is exchanged and stored within such systems, legitimate concerns about the privacy of the stored data occur, as confidential medical data is a promising goal for attackers. These concerns and the lack of existing approaches that provide a sufficient level of security raise the need for a system that guarantees data privacy and keeps the access to health data under strict control of the patient. This paper introduces the new architecture PIPE (Pseudonymization of Information for Privacy in e- Health) that integrates primary and secondary usage of health data. It provides an innovative concept for data sharing, authorization and data recovery that allows to restore the access to the health care records if the patients' security token is lost or stolen. The concept can be used as basis for national EHR initiatives or as an extension to EHR applications.

3. SYSTEM STUDY

3.1 EXISTING SYSTEM:

A fine-grained distributed data access control scheme is proposed using the technique of attribute based encryption (ABE). A rendezvous-based access control method provides access privilege if and only if the patient and the physician meet in the physical world. Recently, a patient-centric and fine-grained data access control in multi-owner settings is constructed for securing personal health records in cloud computing.

Lin et. al. proposed SAGE achieving not only the content-oriented privacy but also the contextual privacy against a strong global adversary. Sun et al. proposed a solution to privacy and emergency responses based on anonymous credential, pseudorandom number generator and proof of knowledge. Lu et al. proposed a privacy-preserving authentication scheme in anonymous P2P systems based on Zero-Knowledge Proof.

3.1.1 Disadvantages of Existing System

- ❖ It mainly focuses on the central cloud computing system which is not sufficient for efficiently processing the increasing volume of personal health information in m-healthcare cloud computing system.
- ❖ Moreover, it is not enough to only guarantee the data confidentiality of the patient's personal health information in the honest-but-curious cloud server model since the frequent communication between a patient and a professional physician can lead the adversary to conclude that the patient is suffering from a specific disease with a high probability.
- ❖ The heavy computational overhead of Zero-Knowledge Proof makes it impractical when directly applied to the distributed m-healthcare cloud computing systems where the computational resource for patients is constrained.

3.2 PROPOSED SYSTEM:

In this paper, we consider simultaneously achieving data confidentiality and identity privacy with high efficiency. In distributed m-healthcare cloud computing systems, all the members can be classified into three categories: the directly authorized physicians with green labels in the local healthcare provider who are

authorized by the patients and can both access the patient's personal health information and verify the patient's identity and the indirectly authorized physicians with yellow labels in the remote healthcare providers who are authorized by the directly authorized physicians for medical consultant or some research purposes (i.e., since they are not authorized by the patients, we use the term 'indirectly authorized' instead).

They can only access the personal health information, but not the patient's identity. For the unauthorized persons with red labels, nothing could be obtained. By extending the techniques of attribute based access control and designated verifier signatures (DVS) on de-identified health information, we realize three different levels of privacy-preserving requirement mentioned above.

3.2.1 Advantages of Proposed System:

- A novel authorized accessible privacy model (AAPM) for the multi-level privacy- preserving cooperative authentication is established to allow the patients to authorizecorresponding privileges to different kinds of physicians located in distributed healthcare providers by setting an access tree supporting flexible threshold predicates.
- Based on AAPM, a patient self-controllable multilevel privacy-preserving cooperative authentication scheme (PSMPA) in the distributed m-healthcare cloud computing system isproposed, realizing three different levels of security and privacy requirement for the patients.
- The formal security proof and simulation results show that our scheme far outperforms the previous constructions in terms of privacy-preserving capability, computational, communication and storage overhead.

3.4 MODULES DESCRIPTION

- SYSTEM MODEL
- SIGNATURE SCHEME
- PSMPA DESIGN

MODULE DETAILSSYSTEM

MODEL

In the first module, we develop the basic e-healthcare system which consists ofthree components: body area networks (BANs), wireless transmission networks and the healthcare providers equipped with their own cloud servers. The patient's personal health information is securely transmitted to the healthcare provider for theauthorized physicians to access and perform medical treatment.

We further illustrate the unique characteristics of distributed m-healthcare cloud computing systems where all the personal health information can be shared among patients suffering from the same disease for mutual support or among the authorized physicians in distributed healthcare providers and medical research institutions for medical consultation.

In our system model, we consider a typical data sharing in cloud-assisted IoT scenario, which mainly includes four types of entities, namely, authentication center (AC), cloud service provider (CSP), data owners and data consumers.

- Authentication center (AC): a critical entity responsible for initializing the system and responding to registration requests from system users (including data owners and data consumers).
- Cloud service provider (CSP): an entity which stores encrypted data (i.e., data in ciphertext format) outsourced from data owners and responds to conversion requests of data owners.
- Data owners: the users who encrypt their data collected from IoT devices and then outsource the resulting ciphertexts to CSP; they can also specify access policies and then delegate CSP to convert the ciphertexts satisfying the access policies so that designated data consumers can access the underlying data.
- Data consumers: the users who retrieve the ciphertexts stored in CSP and recover the underlying data using their private keys.

SIGNATURE SCHEME

We propose a patient self-controllable and multi-level privacy-preserving cooperative authentication scheme based on ADVS to realize three levels of security and privacy requirement in distributed m-healthcare cloud computing system which mainly consists of the following five algorithms: Setup, Key Extraction, Sign, Verify and Transcript Simulation Generation.

In an attribute based designated verifier signature scheme, as to unforgeability, we mean that the adversary wants to forge a signature w.r.t an unsatisfied verifier's specific access structure. The definition of unforgeability allows an adversary not togenerate an effective signature with an access structure.

PSMPA Design

In this module, we give a design of the proposed PSMPA to implement AAPM introduced previously, realizing three different levels of security and privacy requirements. The signing algorithm outputs a signature of the patient's personal health information m which can only be recovered and verified by the directly authorized physicians whose sets of attributes satisfy the access tree. In our proposed PSMPA, for directly authorized physicians, performing the Verify algorithm allows them to both decipher the patient's identity using the private key of the patient's registered local healthcare provider and recover the patient's personal health information m using the authorized attribute private key. Therefore, the unlink ability between the patient identity and his personal health information can still be preserved.

4. CONCLUSION

In this paper, we proposed a cloud-assisted, privacy preserving machine learning classification scheme for resource constrained IoT devices. By introducing an additional cloud server and employing a two-stage decryption Paillier-based cryptosystem, our scheme allows an IoT device to offload expensive classification computations to the cloud server in privacy-preserving manner, thereby ensuring data privacy for both IoT client and machine learning service provider. The extensive complexity analysis and performance evaluation demonstrate that the proposed scheme provides an efficient solution for conducting machine learning on IoT devices, where compared to the existing solutions in the literature.

REFERENCES

[1] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of things in the 5g era: Enablers, architecture, and business models," IEEE Journal on Selected Areas in Communications, vol. 34, no. 3, pp. 510–527, 2016.

[2] L. Yang, Q. Zheng, and X. Fan, "Rspp: A reliable, searchable and privacy-preserving e- healthcare system for cloud-assisted body area networks," in IEEE INFOCOM 2017-IEEE Conference on Computer Communications. IEEE, 2017, pp. 1–9.

[3] S. Dhingra, R. B. Madda, A. H. Gandomi, R. Patan, and M. Daneshmand, "Internet of things mobile-air pollution monitoring system (iotmobair)," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5577–5584, 2019.

[4] J. A. Guerrero-Ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies," IEEE Wireless Communications, vol. 22, no. 6, pp. 122–128, 2015.

[5] Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, "Securing consumer iot in the smart home: architecture, challenges, and countermeasures," IEEE Wireless Communications, vol. 25, no. 6, pp. 53–59, 2018.

[6] W. Wang, P. Xu, and L. T. Yang, "Secure data collection, storage and access in cloud- assisted iot," IEEE Cloud Computing, vol. 5, no. 4, pp. 77–88, 2018.

[7] P. Xu, S. He, W. Wang, W. Susilo, and H. Jin, "Lightweight searchable public-key encryption for cloud-assisted wireless sensor networks,"IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3712– 3723, 2018.

[8] Y. Yahiatene, D. E. Menacer, M. A. Riahla, A. Rachedi, and T. B. Tebibel, "Towards a distributed abe based approach to protect privacy on online social networks," in 2019 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2019, pp. 1–7.

[9] A. Kaci, T. Bouabana-Tebibel, A. Rachedi, and C. Yahiaoui, "Toward a big data approach for indexing encrypted data in cloud computing," Security and Privacy, vol. 2, no. 3, p. e65, 2019.