Document Digitization using IOT

Kiran Ramgade[1], Deepak Dange[2],Pratik M Shinde[3]
[1]BE,Computer Engineering,RMD Sinhgad School of Engineering
[2]BE,Computer Engineering,RMD Sinhgad School of Engineering
[3]BE,Computer Engineering,RMD Sinhgad School of Engineering

Abstract- *The Internet of Things (IoT) have a synergistic effect in the modern organizations as digitization is a new business trend for various industries. Therefore, many organizations outsource their crowd sourced Industrial-IoT (IIoT) data in the cloud system to reduce data management overhead. However, data authentication is one of the fundamental security/trust requirements in such IIoT network. Certificateless signature (CLS) scheme is a cryptographic primitive that provides data authenticity in IIoT systems. Recently, CLS has become a prime research focus due to its ability to solve the key-escrow problem in very recent identity-based signature technique. Many CLS schemes have already been developed using map-to-point (MTP) hash function and random oracle model (ROM). However, due to the implementation difficulty and probabilistic nature of MTP function and ROM, those CLSs are impractical. Hence, the development of a CLS for lightweight devices mounted in IIoT has become one of the most focused research trends. This paper presents a new pairing-based CLS scheme without MTP function and ROM. The new CLS is secure against both the Type-I and Type-II adversaries under the hardness of Extended Bilinear Strong Diffie-Hellman (EBSDH) and Bilinear Strong Diffie-Hellman (BSDH) assumptions, respectively. Performance evaluation and comparison proves that our scheme outperforms other CLS schemes.*

Keywords- Certificateless signature; Industrial Internet of Things; Provable security; Cryptography; Bilinear pairing.

I. INTRODUCTION

In present-day, the Internet of Things (IoT) influences the neoteric society by raising the potential migration without compromising human daily needs, improving personal security through surveillance and making physical environments more user-friendly. The idea of IoT was coined in 1999 by Ashton during his extensive research on the Radio Frequency Identification (RFID) [1]. Basically, IoT provides a self-establishing network of highly coupled heterogeneous objects, namely, different smart devices, RFID, sensors, actuators, etc. Such smart devices simplify the retrieval as well as the exchange of data in various applications [1]. The IoT brings a pervasive digital appearance by engaging society and industries, and it enables a series of interactions between human-to-human, human-to-thing, thing-to-thing or thing-to-things.

IoT has a significant demand for the technological infrastructure as the organizations today are subjected to multiple thrusts from different fields. Faster replies at considerable costs, scalable and agile operations are some of the prospective requirements from IT infrastructure leading to increased demands on the Internet. Many industries exploit the concept of IoT and use it across the various business sectors such as manufacturing, logistics, etc. This is known as Industrial IoT (IIoT) where employees use their smart devices to perform many business-related activities through an active Internet [4], [5]. The data needed in various IIoT settings are being retrieved by introducing the methodology of crowdsourcing nowadays as it reduces data management overhead by collecting the task from active users connected to the Internet.

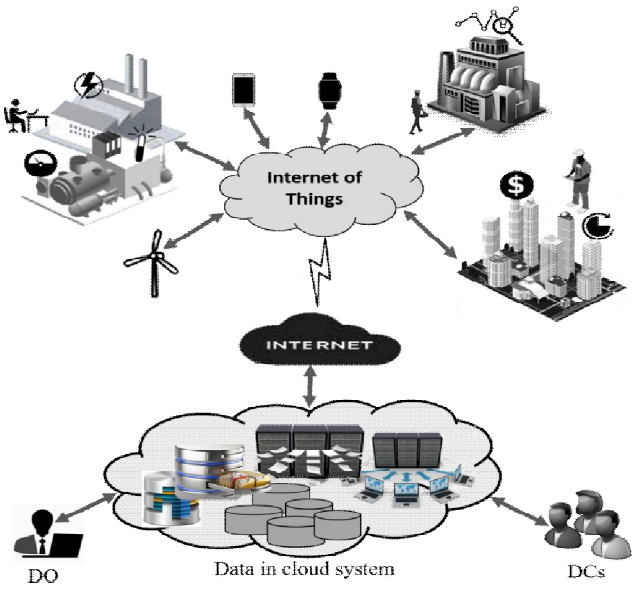

Fig. 1. Cloud-centric IIoT data storage architecture

II. PRELIMINARIES

This section discusses the structure and security notion of CLS with some cryptographic definitions. In addition, a list of symbols used throughout the paper is summarized in Table I

Symbols	Meaning
P	Sufficiently large prime number
tt_1, tt_2	Cyclic groups of same order p
G	Generator of tt_1
$H(\cdot)$	Cryptographic hash functions: $H: \{0,1\}^* \rightarrow Z_p$
MSK	Private key of the KGC
$params$	Public parameters of the KGC
Id_i	i-th user identity
X_i	Secret value selected by the user Id_i
D_i	The partial private key of user i
Y_i	The public key of user i
M	The message in Z_p^*
Σ	Signature of message m
$e(\cdot, \cdot)$	The bilinear pairing $e: tt_1 \times tt_1 \rightarrow tt_2$

Signature generation and verification. In addition, we also discuss how our scheme is efficient than others from its implementation point of view later in this section.

Computational time: The cost of Setup algorithm comprises the generation of a prime ordered group pair

A. Mathematical definitions

This section discusses some of the hard assumptions, which are considered to be intractable by all probabilistic polynomial time (PPT) algorithms.

Definition 1 (Negligible function): A function s(y) is said negligible if, ν > 0, y0 y0. Such that s(y) ≤ 1 holds ∀ y ≥.

Definition 2 (Cryptographic Hash Function): It is hard for every PPT algorithm A to find out x for a given value of $H(x)$. The advantage s of in finding another solution x^j is considered as

$$\Pr\left[x \in_R \{0,1\}^* \, . \, x^j \leftarrow A(y) \right] \geq s$$

Definition 3 (Computational Diffie-Hellman Assumption): Given a tuple $T = (g, g^x, g^y)$ it is computationally hard for any PPT algorithm A to compute $X = g^{xy}$ without the knowledge of $x, y \in_R Z_p^*$. The advantage s of the algorithm in finding the solution is considered as

$$\Pr\left[g \in_R tt_1, \; x, y \in_R Z_p^* \; . \; T = (g, g^x, g^y) \; . \; X \leftarrow A(T) \; . \; X = g^{xy} \right] \geq s$$

Definition 4 (Bilinear Strong Diffie-Hellman Assumption): For every PPT algorithm , calculating $Y = (k, e(g, g)^{\frac{1}{x+k}})$ from known $T = (g, g^x, g^{x^2}, \ldots, g^{x^q})$ is very hard for known k, and $x, k \in_R Z_p^*$.

Performance analysis

This section discusses the performance of our CLS scheme from the aspect of the security type, security definition, signature length with the computational complexity during (tt1, tt2), two exponentiations and a pairing computation; Set-Partial-Private-Key algorithm needs two exponentiation cost computations, and Set-Public-Key algorithm computes one exponentiation cost.

III. CONCLUDING REMARKS

The IIoT with cloud technology is transforming our society and the industries into a new digital form globally by adding many extra facilities. Therefore, promising the authenticity of IIoT data is one of the important issues for any IIoT System. To address this issue, a novel CLS technique using bilinear pairing applicable for IIoT environments is presented in this paper. The proposed CLS resists both Type-I and Type-II attacks under the intractability of EBSDH and BSDH problems without considering the random oracle model respectively. In addition, our scheme takes lesser cryptographic operations and avoids probabilistic MTP hash function. Both the theoretical and practical experiments show that our CLS scheme is com- putationally efficient and has better security features compared to other existing CLSs. Thus, our CLS scheme is applicable in every scenario, especially where the computational cost is a major issue and the communication bandwidth, as well as storage space, is confined. Thus, our lightweight CLS is compatible with the IIoT system than other CLS schemes.

REFERENCES

[1] Kevin Ashton. That 'internet of things' thing. RFiD Journal, 22(7), 2009.

[2] Gartner says 8.4 billion connected. http://www.gartner.com/newsroom/ id/3598917. Accessed: 2017-02-07.

[3] Mimi Ma, Debiao He, Neeraj Kumar, Kim-Kwang Raymond Choo, and Jianhua Chen. Certificateless searchable public key encryption scheme for industrial internet of things. IEEE Transactions on Industrial Informatics, 2017.

[4] Xiong Li, Jieyao Peng, Jianwei Niu, Fan Wu, Junguo Liao, and Kim- Kwang Raymond Choo. A robust and energy efficient authentication protocol for industrial internet of things. IEEE Internet of Things Journal, 2017.

[5] Xiong Li, Jianwei Niu, Md Zakirul Alam Bhuiyan, Fan Wu, Marimuthu Karuppiah, and Saru Kumari. A robust ecc based provable secure authentication protocol with

privacy preserving for industrial internet of things. IEEE Transactions on Industrial Informatics, 2017.

[6] Mohamed Almorsy, John Grundy, and Ingo Mu¨ller. An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107, 2016.

[7] Adi Shamir. Identity-based cryptosystems and signature schemes. In Advances in cryptology, pages 47–53. Springer, 1984.

[8] Sattam S Al-Riyami and Kenneth G Paterson. Certificateless public key cryptography. In Advances in cryptology-ASIACRYPT 2003, pages 452–473. Springer, 2003.

[9] Boyang Wang, Baochun Li, Hui Li, and Fenghua Li. Certificateless public auditing for data integrity in the cloud. In Communications and Network Security (CNS), 2013 IEEE Conference on, pages 136–144. IEEE, 2013.

[10] Zhe Liu, Xinyi Huang, Zhi Hu, Muhammad Khurram Khan, Hwajeong Seo, and Lu Zhou. On emerging family of elliptic curves to secure internet of things: Ecc comes of age. IEEE Transactions on Dependable and Secure Computing, 14(3):237–248, 2017.