ID-based Strong Designated Verifier Signature Scheme and its Applications in Internet of Things

Mohammad Beheshti-Atashgah
Electrical and Computer Engineering Complex
Malek-Ashtar University of Technology
Tehran, Iran
m_beheshti_a@mut.ac.ir

Mohammd Reza Aref
Department of Electrical Engineering
Sharif University of Technology
Tehran, Iran
aref@sharif.edu

Majid Bayat
Department of computer Engineering
Shahed University
Tehran, Iran
mbayat@shahed.ac.ir

Morteza Barari
Electrical and Computer Engineering Complex
Malek-Ashtar University of Technology
Tehran, Iran
m.barari@mut.ac.ir

***Abstract*—Strong designated verifier signature scheme is a concept in which a user (signer) can issue a digital signature for a special receiver; i.e. signature is produced in such way that only intended verifier can check the validity of produced signature. Of course, this type of signature scheme should be such that no third party is able to validate the signature. In other words, the related designated verifier cannot assign the issued signature to another third party. This article proposes a new ID-based strong designated verifier signature scheme which has provable security in the ROM (Random Oracle Model) and BDH assumption. The proposed scheme satisfies the all security requirements of an ID-based strong designated verifier signature scheme. In addition, we propose some usage scenarios for the proposed schemes in different applications in the Internet of Things and Cloud Computing era.**

***Index Terms*—ID-based signature scheme; designated verifier signature; Intenet of Things; Smart home; Cloud; provable security; bilinear pairing.**

I. Introduction

The IoT (Internet of Things) describes a concept of a large scale network in which various devices and things are highly connected together. The IoT contains different types of devices; for example: smartphones, sensors, computers, RFIDs, actuators, etc. All these devices have various functionality and capability, and also are different in terms of scales, computing power and memory. The main issue of the IoT is how to utilize the common internet platform to implement the concept of the internet of things. In this regard, researchers have focused an areas such as design, implementation, adoption and applications of standard protocols on the IoT [1]. According to Gartner's estimates [2], the number of connected devices (things) in the IoT, including smartphones, tablets, sensors and etc, will reach to more than 26 billion units in 2020.

In general, the internet of things have several significant features, which makes the IoT usable in almost every area. Some of these features are as follows: ubiquitous property; sensing and collecting data and information about different parameters; feature to rise the quality of everyday life; and these useful features make the internet of things directly affect the society and economy. Also, the IoT covers various application areas: social, personal, environmental, medical, military, logistics and etc. In an incomplete division, internet of things' applications are classified into three main domains: (I) industrial domain, (II) smart city domain and (III) ehealth domain [3].

In this article, we want to propose an Identity based strong designated verifier signature scheme (ID-SDVSS). Moreover, we also propose examples of application scenarios of the schemes in order to use smart homes which are a subset of the smart cities domain.

In a typical city, buildings/homes are equipped with many smart devices and embedded sensors (e.g. mobile phones, laptops, smart TVs, PCs, lights, cameras, plugs, appliance and etc) that integrated with different types of communication technologies within homes and buildings, create a wide range of different types of applications. Since allow to remotely control every-things via internet and web apps, HAS (Home Automation Systems) are particularly attractive. Some usages utilize the easiest and simplest abilities enable by the Internet of Things (IoT), such as applications that are use for security purposes (e.g. accesss control, intrusion detection systems and visual surveillance), for plant maintenance and management (i.e. asset maintenance/management across the home, fault detection systems), entertainment systems (i.e. multimedia distribution across the home), service automation systems (i.e. lighting, HVAC, irrigation). Other different types of applications are unified with the smart grids and optimize homemade/indoor energy consumption [4]. For instance, the HAN (Home Area Network) also allows appliances/devices to communicate with smart meters till to decrease costs while providing the needed performance. This can be gained through services that schedule the different activities of hosehold appliances/devices (for ex-

This work was partially supported by Iranian-NSF under grant No. 96.53979.

978-1-7281-1508-5/19/$31.00 ©2019 IEEE

ample, dishwasher cycle/washing machine) in an intelligent way avoiding the expensive peak periods. More modern applications can allow to the smartphones/tablets as the remote controls to manipulate all the home appliances/devices (e.g. in order to turn off appliances/devices when not used) and to control/monitor habits of users [5] by tracing their phones to make everyday life/home living easier and more comfortable. For instance, through information analysis, the system will learn the exact time when a person/host arrives at his/her home, therefore opening the doors, turning up the different lights and powering on the water boiler to fill the bathtub. Such these automatic systems can be reschedules/canceled by the relevant user at any time of day.

A. Related Work

In an ordinary digital signature scheme, anyone can check the validity of a signature using the signer's public key and verification algorithm and providing accuracy, verify it. However, in some usages and scenarios, it is needed that the digital signature has a special property which only is verifiable by a specific person (i.e. designated verifier). This is a particular possibility which is provided by DVS scheme. Jakobsson et al. first proposed the concept of designated verifier signature scheme in 1996 [6]. In a designated verifier signature scheme, a signer signs a message such that only a specific receiver can validate it. In this case, the designated verifier is not able to prove the validation of the respective signature to a third party. These types of signatures have many applications such as e-voting protocols, e-commerce, software licensing and etc.

In 2003, Saeednia et al. described the concept of strong designated verifier signature scheme based on Jakobsson's scheme which in their scheme, no third party can verify a signature since the designated verifier's private key is required in the verifying phase [7]. After Jakobsson's scheme and Saeednia's scheme, many designated verifier signature schemes have been proposed that most of these schemes are identity-based signature schemes [8], [9], [10], [11] and [12]. These types of signatures are result of the combining the ID-based cryptography and designated verifier digital signature schemes. These signatures have the following security requirements [13]: Unforgeability, Correctness, Strongness, Non-transferability and Source hiding. The first ID-based designated verifier signature scheme was proposed by Susilo et al. in 2004 ([10]). Lipma et al. showed that Saeednia et al.'s scheme was vulnerable against delegatability attack [14]. In other words, in Saeednia et al.'s scheme, a signer can delegate his/her signing capability to a third party without disclosing his/her private key. Recently, Zhang and Mao proposed a new ID-based strong designated verifier signature scheme (we will show it with Zhang scheme) based on bilinear pairings. They claimed that their scheme satisfies the source hiding property [15]. In 2009, Kang et al. showed that Zhang's scheme cannot satisfy the strong designated verifier property; that is anyone who intercepts a signature can get some information and subsequently verify a new signature without the designated verifier's private key. They proposed an improvement of Zhang's scheme in their paper and claimed that their proposed scheme was strong and unforgeable [16]. Kang et al. also proposed other scheme which consists of a new ID-based designated verifier signature scheme with its provable security [17]. But, Lee et al. showed that Kang et al.'s scheme cannot satisfy these security properties: Non-Delegatability, Unforgeability and Strongness [18]. Moreover, Du and Wen showed that the Kang et al.'s scheme is universally forgeable [19]. Based on the Gentry-Silverberg hierarchical identity-based encryption scheme, in 2011, Huang et al. proposed a new ID-based strong designated verifier signature scheme. However, their scheme has relatively long signature size and also is not appropriate in systems/applications where bandwidth is restricted [20].

In 2013, Duan et al. proposed an improved identity-based strong designated verifier scheme with short signature size and provide formal proof based on the CDH assumption [21]. Their scheme was proposed based on the Kang et al.'s scheme ([17]) and offered it's provable security in the random oracle model ([19]). In 2014, Wang proposed a signer-admissible identity-based strong designated verifier signature scheme with the acceptable length of sign [22]. In 2015, Islam and Biswas proposed a pairing-based strong designated verifier signature scheme with message recovery along with its provable security. However, Hu et al.'s showed that Islam and Biswas' scheme ([23]) suffers from two types of delegatability attacks. They also proposed a new scheme [24] that overcome the problems existed in their scheme. In 2017, they also proposed another strong designated verifier signature scheme scheme with undeniability property [25]. In the same year, Khan et al. proposed a new strong short designated verifier signature scheme; they claimed that their proposed scheme is a efficient and secure scheme but they did not provide any provable security for their scheme [26]. Additionally, Chen et al.'s proposed an efficient strong designated verifier signature scheme which satisfied non-delegatability property [28]. Recently, Rastegari et al. have proposed a new universal designated verifier signature scheme in the standard model [29]. Also, Li et al. provided an universal forgery attack against Zhang et al.'s scheme [30] and proposed a new improved scheme [31].

In this paper, we want to propose a new Id-based designated verifier signature scheme which has provable security in the random oracle model and based on the bilinear Diffie-Hellman problem (BDH). We also show that our scheme is also efficient by the comparison among other existing schemes.

B. Our contribution

In this work, we present a new strong designated verifier signature scheme (SDVSS). Our proposed construction of SDVSS satisfies these security requirements: Non-Transferability, Non-delegatability and Source hiding. Furthermore, we introduce a formal security analysis that proves the security of the proposed SVDSS in the random oracle model and based on the hardness of BDH problem. Additionally, in the form of a table, we compare the proposed SDVSS with other previous schemes from the point of view of efficiency and computational complexity. Finally, we describe some applicable scenarios

of the proposed scheme in the internet of things and cloud computing era.

C. Outline

This rest of this study is organized as follows: In the next section, we review some needed preliminaries. During Section3, we propose a novel Identity-based designated verifier signature scheme. The provable security analysis of our proposed scheme in ROM (random oracle model) is discussed in Section 4, along with a comparison between our proposed scheme and other existing schemes. In Section 5, we offer some usage scenarios of proposed IBDVS and IBDVPS schemes in cloud and smart homes. Section 6 contains our concluding remarks.

II. Preliminaries

During this section, we want to briefly review some related concepts and needed mathematical backgrounds.

A. Bilinear Pairings

Assume that G_1 and G_2 be additive cyclic group and multiplicative cyclic group with prime order q, respectively.Let that P be a generator of G_1. We say that the map $e: G_1 \times G_1 \to G_2$ is a bilinear pairing if it satisfies the following conditions:

1) Bilinearity: $e(aP,\ bQ) = e(P,\ Q^{ab}$ for all $P,\ Q \in G_1$ and $a,\ b \in \mathbb{Z}_q^*$.
2) Non-degeneracy: There exist $P \in G_1$ and $Q \in G_1$ such that $e(P,\ Q) \neq 1$.
3) Computability: There exist an algorithm to effectively compute $e(P,\ Q)$ for all $P,\ Q \in G_1$.

B. Definitions

Definition 1 (Bilinear Diffie-Hellman Problem). For a given randomly $P \in G_1$ and also aP, bP and cP (for unknown chosen $a, b, c \in \mathbb{Z}_q$ at random), the BDH problem is to compute $e(P,\ P)^{abc}$.

Definition 2 (Bilinear Diffie-Hellman Assumption). If g is a Bilinear Diffie-Hellman (BDH) parameter generator, then the advantage $\mathrm{Adv}_g(\mathcal{A})$ (that an adversary $\mathcal{A}$ has in solving the Bilinear DH problem) is defined to be the probability that the algorithm $\mathcal{A}$ takes the parameters $G_1,\ G_2,\ e,\ P,\ aP,\ bP,\ cP$ as its inputs and outputs $e(P,\ P)^{abc}$ where $G_1,\ G_2,\ e$ is the output of g for sufficiently large security parameter $k,\ P$ is a random generator of G_1 and a, b, c are randomly chosen from $\mathbb{Z}_q$. The Bilinear Diffie-Hellman (BDH) assumption is that $\mathrm{Adv}_g(\mathcal{A})$ is negligible for all efficient algorithms $\mathcal{A}$.

Definition 3 (Non-Transferability). We say a DVSS would be non-transferable if the issued signature that generated by the signer himself/herself is indistinguishable from the signature generated by the related designated verifier from a computational point of view.

Definition 4 (Privacy of Signer). A DVS scheme has the Privacy preserving of Signer if there is no distinguisher $\mathcal{D}$ which runs in time at most t, asks at most q_{Sign} queries to $\mathcal{O}_{Sign}$, at most q_{Sim} queries to $\mathcal{O}_{Sim}$, and at most q_{Ver} queries to $\mathcal{O}_{Ver}$, and wins the above game with probability that deviates from one-half by more than ϵ [27].

Definition 5 (Non-Delegatability). A DVS scheme has the non-delegatability property if an adversary, even knowing the private key of a signer (like Alice) or designated verifier (like Bob), still cannot produce a valid signature on a message.

III. The Proposed Identity-based Designated Verifier Signature Scheme

The proposed IDVSS has the following five phases:

1. Setup: In this phase, PKG randomly chooses two groups G_1 and G_2 of same prime order q. G_1 is a Gap Diffie-Hellman group and G_2 is a multiplicative group. PKG also picks a bilinear map like $e: G_1 \times G_1 \to G_2$, and an desired generator like $P \in G_1$. Then, it randomly picks a value $s \in \mathbb{Z}_q^*$ as its master key and also computes the corresponding public key $P_{\mathrm{pub}} = sP$. $H_1(\cdot)$ and $H_2(\cdot)$ are two one-way cryptographic hash functions with $H_1: \{0,\ 1\}^* \to G_1$ and $H_2: \{0,\ 1\}^* \to \mathbb{Z}_q^*$. The set $(G_1,\ G_2,\ P,\ P_{\mathrm{pub}}, H_1,\ H_2,\ e,\ q\ )$ are system parameters and s is the master key.

2. KeyExtract: For an identity ID, PKG computes $S_{ID} = sH_1(ID)$ as the private key and returns it to the related user with identity ID. We remark $Q_{ID} = H_1(ID)$ as the public key of the user with identity ID. In this scenario, Alice (with identity ID_A) has public key $Q_A = H_1(ID_A)$ and secret key $S_A = sQ_A$. Bob similarly (with identity ID_B) has public key $Q_B = H_1(ID_B)$ and secret key $S_B = sQ_B$.

3. Sign: In order to sign a message m for Bob, signer (i.e. Alice) chooses one number $r \in \mathbb{Z}_q^*$ at random and computes the following terms:

$$U = rS_{ID_A},\ h = H_2(m,\ U) \tag{1}$$

$$T = H_2(m,\ U)\, S_{ID_A} = hS_{ID_A} \tag{2}$$

$$\sigma = e(T,\ Q_{ID_B}) \tag{3}$$

Alice (signer) sends $(\sigma,\ U)$ to Bob (designated verifier) as the signature on the message m.

4. Verify: Upon receiving the signature$(\sigma,\ U)$, Bob firstly computes $h = H_2(m,\ U)$. Then, he accepts the signature as a valid one if and only if the following equation is established.

$$\sigma = e(T,\ Q_{ID_B}) = e(hQ_{ID_A},\ S_{ID_B}) \tag{4}$$

5. Transcript Simulation: The designated verifier (Bob) randomly picks a value $r' \in \mathbb{Z}_q^*$ and then calculates:

$$U' = r' S_{ID_A},\ h' = H_2(m,\ U') \tag{5}$$

$$T' = H_2(m,\ U')S_{ID_B} = h' S_{ID_B} \tag{6}$$

$$\sigma' = e(T',\ Q_{ID_A}) \tag{7}$$

Correctness:

$$\begin{aligned} \sigma' &= e(T',\ Q_{ID_A}) = e(h' S_{ID_B},\ Q_{ID_A}) \\ &= e(sh' Q_{ID_B},\ Q_{ID_A}) = e(sh' Q_{ID_A},\ Q_{ID_B}) \\ &= e(h' Q_{ID_A},\ S_{ID_B}) \end{aligned}$$

and

$$\sigma = e\left(hQ_{ID_A},\ S_{ID_B}\right)$$

Obviously, the signature $(\sigma^{'},\ U^{'})$ satisfies the verification phase.

IV. Evaluation of the proposed scheme

In this section, we give four types analysis during four following subsections. First of all, we show that our proposed scheme is unforgeable. After that, we will discuss other security requirements. Then, we give privacy analysis of our proposed scheme and Finally, we give performance analysis of the presented ID-SDVSS.

A. Security and privacy analysis

In this subsection, we want to give security evaluation of the proposed ID-SDVS scheme. we present the security results of the scheme through the following theorem.

Theorem 1. (*Unforgeability of ID-SDVS*) If there exists an attacker (adversary) like $\mathcal{A}$ which can break the proposed scheme, then there exists a simulator $\mathcal{B}$ which is able to solve the Bilinear Diffie-Hellman (BDH) problem with a non-negligible probability.

Proof. Due to the page limitation, the proof has been omitted.■

Theorem 2. (*Non-Transferability of ID-SDVSS*) The proposed ID-SDVS scheme is a non-transferable against public key PPT distinguisher and an adaptive chosen message.

Proof. Due to the page limitation, the proof has been omitted.■

In this subsection, we show that the proposed IDVS scheme protects the privacy of signer's identity; i.e. the proposed scheme provides the feature of signer's identity privacy preserving. We propose this property in the form of the following theorem.

Theorem 3. If there exists an attacker $\mathcal{A}$ which can break the proposed scheme, then there exists a simulator $\mathcal{B}$ which can solve the BDH problem with non-negligible probability.

Proof. Due to the page limitation, the proof has been omitted.■

Theorem 4. (*Non-Delegatability of ID-SDVSS*) The proposed ID-SDVS scheme satisfies the non-delegatability property.

Proof. In the our proposed scheme, both of Alice's (i.e. signer) private key and Bob's (i.e.designated verifier) private key are required in the signing and the verification phases. Even if the common parameter $e(Q_{ID_A},\ S_{ID_B})$ is transferable to a third party, he/she is not able to produce a valid signature on a message like m. Because, in order to produce a valid signature on a message, he simultaneously needs Alice and Bob's private keys, and with the possession of a private key cannot generate a valid ID-SDVSS signature on a message m. Therefore, the proposed scheme satisfies the non-delegatability feature. ■

B. Performance analysis

In this subsection, we show a performance comparison of the proposed scheme with other well-known schemes based on the required computational costs and the length of the issued signature. Let C_p be pairing operation, C_* be multiplication in group G_1 and C_e be exponentiation in group G_2. C_h be hash operation and C_i be inverse operation. In addition, suppose that C_s be symmetric encryption/decryption operation. Note that add operations in G_1 are be neglected. We suppose that the bit length of element in G_1 is $|G_1|$ (we consider that $|G_1| = |G_2|$). Table I shows that on the whole, the proposed scheme is more efficient than four firs schemes. Compared to the Kang et al.'s scheme, the proposed ID-SDVS scheme has only two additional multiplications (one in the signing phase and other in the verifying phase) which due to the higher security of the proposed scheme, this computational cost is assumed negligible. Moreover, a brief security comparison of the proposed scheme and other schemes has been showed in Table I.

V. Application of the Proposed Signature Schemes in IoT Era

A. Application in Cloud data auditing

As described in [32] our proposed DVS scheme can be used for data auditing in the Clouds. Like Worku et al.'s plan, Our scheme has three entities for use in a cloud data auditing system. These entities are as follows: user (U) who has huge amount of data for storage; cloud service provider (CSP) that provide relevant services for its users; and the designated verifier (DV) that checks the validity of the user's data. The user and CSP are potential signature holders and they are able to designate a specific verifier for the auditing system. Moreover, whenever user or cloud service provider wants to replace a verifier, we suppose that he/she negotiate together and agree on the another verifier. Our scenario has three phases (shown in Fig. 1): System initialization, Audit delegation and Challenge-response protocol for auditing.

The system initialization phase: This phase includes three algorithms namely Setup, KeyGen and SignGen. Setup is a probabilistic polynomial time algorithm that takes the related security parameter and outputs the public parameters of system. KeyGen takes the public parameters and outputs public/private keys (sk_S, pk_S) and (sk_V, pk_V) for the user and designated verifier, respectively. SigGen is also a deterministic polynomial time algorithm that generate a signature σ.

The audit delegation phase: This is a verifier designation algorithm that takes the signature σ and designated verifier publc key pk_V as inputs and outputs a designated verifier signature $\widehat{\sigma}$.

The challenge-response phase: This phase consists of the three algorithms: ChalGen, ProofGen and VerProof. ChalGen is a random algorithm that takes the public parameters as input and outputs an appropriate challenge (Chal). ProofGen takes the pubic parameters, user data, signature σ challenge Chal as its inputs and outputs the proof P to designated verifier for user data verification. VerProof is a deterministic randomized algorithm run by designated verifier in polynomial time to control the validity of P generated by cloud service provider. This algorithm takes the private key of designated verifier, challenge Chal and proof P, and outputs the verification result

TABLE I
PERFORMANCE COMPARISON BETWEEN THE PROPOSED SCHEME WITH OTHER WELL-KNOWN SCHEMES.

Scheme	Length of signature	Signing cost	Verifying cost
Susilo-scheme [10]	$2\|G_1\| + \|H\|$	$1C_p + 1C_e + 2C_* + 1C_h + 1C_i$	$2C_p + 2C_e + 1C_* + 1C_h$
Kumar-scheme [9]	$4\|G_1\|$	$1C_p + 5C_* + 1C_h + 1C_i$	$4C_p + 1C_h$
Zhang-scheme [15]	$3\|G_1\|$	$4C_* + 1C_h + 1C_i$	$3C_p + 1C_h$
Kang-scheme [16]	$2\|G_1\|$	$1C_p + 1C_* + 1C_h$	$1C_p + 1C_h$
Kang-scheme [17]	$2\|G_1\|$	$2C_p + 1C_e + 2C_* + 1C_h$	$1C_p + 1C_e + 1C_* + 1C_h$
Duan-scheme [21]	$2\|G_1\| + \|\mathbb{Z}_q\|$	$1C_p + 1C_* + 1C_h$	$2C_p + 1C_* + 1C_h$
Chen-scheme [12]	$\|G_1\| + \|\mathbb{Z}_q\|$	$1C_p + 1C_* + 2C_h$	$2C_p + 1C_* + 2C_h$
Wang-scheme [22]	$2\|\mathbb{Z}_q\|$	$1C_p + 1C_e + 1C_* + 1C_i + 2C_h$	$1C_p + 3C_e + 1C_* + 1C_h$
Huang-scheme [20]	$4\|G_1\| + 3\|\mathbb{Z}_q\|$	$4C_p + 3C_e + 2C_* + 5C_h$	$1C_p + 1C_i + 2C_h$
Islam-scheme [23]	$2\|G_1\| + \|\mathbb{Z}_q\|$	$2C_p + 1C_e + 1C_* + 2C_h$	$2C_p + 2C_h$
Hu-scheme [24]	$5\|\mathbb{Z}_q\|$	$3C_e + 2C_* + 2C_h$	$4C_e + 2C_* + 2C_h$
Hu-scheme [25]	$\|G_1\| + 4\|\mathbb{Z}_q\|$	$6C_e + 2C_* + 3C_h$	$9C_e + 3C_* + 1C_h$
Khan-scheme [26]	$\|G_1\| + \|\mathbb{Z}_q\|$	$2C_e + 1C_* + 1C_h$	$2C_e + 1C_* + 1C_h$
Chen-scheme [28]	$\|G_1\| + 2\|\mathbb{Z}_q\|$	$1C_p + 3C_* + 2C_h$	$1C_p + 3C_* + 2C_h$
Rastegari-scheme [29]	$2\|G_1\|$	$3C_p + 3C_e + 10C_*$	$2C_p + 2C_e + 5C_*$
Zhang-scheme [30]	$2\|G_1\|$	$1C_p + 1C_e + 2C_h$	$1C_p + 1C_e + 3C_h$
Li-scheme [31]	$2\|G_1\|$	$C_p + C_s + 3C_h$	$C_p + C_s + 2C_h$
Proposed scheme	$2\|G_1\|$	$1C_p + 2C_* + 1C_h$	$1C_p + 1C_* + 1C_h$

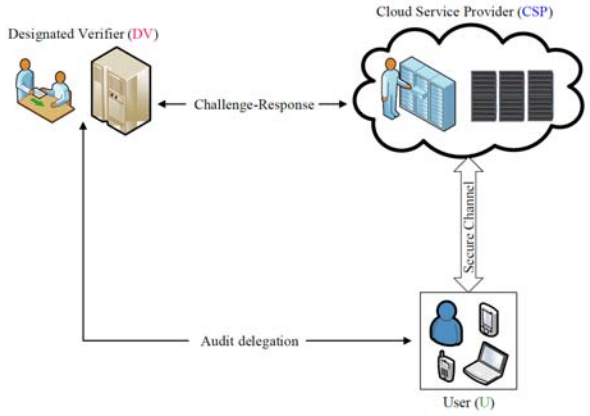

Fig. 1. Cloud data storage and audit architecture.

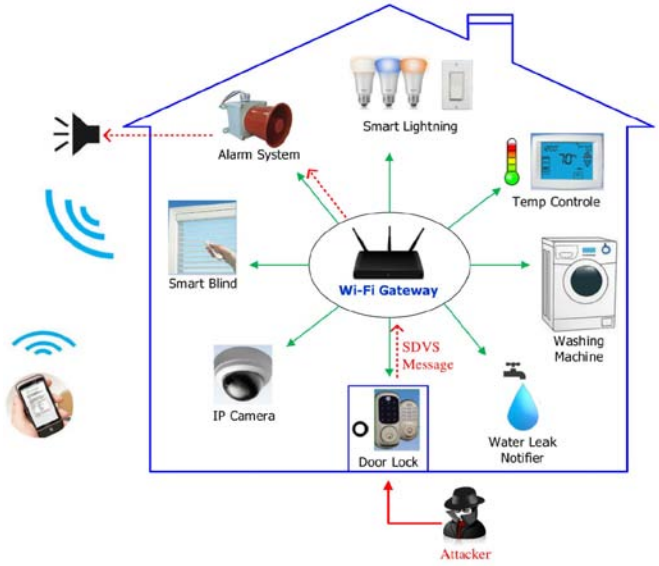

Fig. 2. SDVSS application in the Smart Home.

either 0 or 1, where 0 means failure and 1 means the verification procedure is proved that the file is being stored on the server side correctly.

B. Application Scenario for the DVSS in Smart Home

As explained earlier, in a smart home, a home owner has ability to use (for example) his/her smartphone as an integrated remote control and thus he/she can control and manage all IoT devices and household appliances. In particular, in the ZigBee smart home system, all the smart devices connected to the internet via a Wi-Fi Router. In fact, they communicate with each other through the wireless router and this router handles all communications between the user and all appliances. In this case, the user has a custom App in his/her mobile phone that can communicate with his/her home's router via that App.

Consider the case where the door's sensor of home detects an authorized attempt to enter the home. At this time, the sensor of door should send an alert message to the warning system. For this purpose, the sensor sends its message to the warning system via wireless router. Note that, the sensor's alert message will be released to the public. The sensor can sign its alert message by using the proposed ID-SDVS scheme and then sends it to the warning system. In this case, all the unauthorized things outdoors can probably receive the alert message, but due to the use of SDVSS, none of them can verify that message.

VI. Conclusion

Designated verifier (DV) signature schemes are special types of digital signatures in which, verifier been specified and he/she can only control/check the validity of an issued signature. In this paper, we proposed a new ID-based designated verifier signature scheme (ID-SDVSS) with a proof of its security and also a new ID-based designated verifier proxy signature scheme (ID-SDVPSS). The proposed scheme is efficient and satisfies the all security requirements for a DVSS.

Acknowledgments

This work was partially supported by Iranian-NSF under grant No. 96.53979. The authors would like to thank for its support.

References

[1] K.-T. Nguyen, M. Laurent, N. Oualha, "Survey on secure communication protocols for the Internet of Things", Ad-hoc Networks, pp. 1–15, 2015.
[2] Gartner Inc., "Forecast: The Internet of Things", Worldwide, 2013.
[3] E. Borgia, "The Internet of Things vision: Key features, Applications and open issues", Computer Communications, pp. 1–31, 2014.
[4] J. Lu, T. Sookoor, V. Srinivasan, G. Gao, B. Holben, J. Stankovic, E. Field, K, Whitehouse, "The smart thermostat: using occupancy sensors to save energy in homes", —In: Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems (SenSys'10), pp. 211—224, 2010.
[5] C. Chen, D.J. Cook, A.S. Crandall, "The user side of sustainability: modeling behavior and energy usage in the home", Pervas. Mob. Comput. 9(1), pp. 161—175, 2013.
[6] S.-K. Jakobsson, R. Impagliazzo., "Designated verifier proofs and their applications", In: Advances in Eurocrypt'96. LNCS, 1070. Springer-Verlag, pp. 143-–54, 1996.
[7] S. Saeednia, S. Kramer, O. Markovitch, "An efficient strong designated verifier signature scheme", In: ICISC 2003, Berlin: Springer-Verlag, pp. 40—54, 2003.
[8] X. Huang, W. Susilo, Y. Mu, F. Zhang, "Short designated verifier signature scheme and its identity-based variant", International Journal of Network Security 6(1), pp. 82-–93, 2008.
[9] K. Kumar, G. Shailaja, A. Saxena, "Identity based strong designated verifier signature scheme", Cryptography eprint Archive Report 2006/134. Available at http://eprint.iacr.org/complete/2006/134.pdf.
[10] W. Susilo, F. Zhang, Y. Mu, "Identity-based strong designated verifier signature schemes", In: ACISP 2004. LNCS 3108, pp. 313–324, 2004.
[11] S. Lal, V. Verma, "Identity base strong designated verifier proxy signature schemes", Cryptography eprint Archive Report 2006/394. Available at http://eprint.iacr.org/complete/2006/394.pdf.
[12] G. Chen and Sh. Wan, "Analysis and improvement of identity-based designated verifier signature scheme", 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), pp. 2388–2391, 2012.
[13] J.-S. Lee, J.-H. Chang, D.-H. Lee, "Forgery attacks on Kang et al.'s identity base strong designated verifier signature scheme and its improvement with security proof", Computer and Electrical Engineering, 36, pp. 948–954, 2010.
[14] H. Lipma, G. Wang, F. Bao, "Designated verifier signature schemes: attacks, new security notions and new construction", In: ICALP 2005, LNCS 3580, Springer-Verlag, pp. 459–471, 2005.
[15] J. Zhang, J. Mao, "A novel ID-based designated verifier signature scheme", Information Sciences, 178, pp. 733-–66, 2008.
[16] B. Kang, C. Boyd, E.Dawson, "Identity-based strong designated verifier signature schemes: attacks and new construction", Computer and Electrical Engineering, 35, pp. 49–53, 2009.
[17] B. Kang, C. Boyd, E.Dawson, "A novel identity-based strong designated verifier signature scheme", The Journal of Systems and Software, 82, pp. 270–273, 2009.
[18] J. Lee, J. Chang and D. Lee, "Forgery atacks on Kang et al.'s identity-based strong designated verifier signature scheme and its improvement with security proofs", Computers and Electrical Engineering (36), pp. 948–954, 2010.
[19] H.Du, Q. Wen, "Attack on Kang et al.'s Identity-Based Strong Designated Verifier Signature Scheme", Cryptography eprint report 2006/134. International Association for CryptologicResearch, http://eprint.iacr.org/complete/2006/134.
[20] Q. Huang, G. Yang, D.-S. Wang and W. Susilo, "Identity-based strong designated verifier signature revisited", The Journal of Systems and Software (84), pp. 120–129, 2011.
[21] M. Duan, J. Xu and D. Feng, "Efficient identity-based strong designated verifier signature schemes", Security and Communication Networks (6), Wiley, pp. 902–911, 2013.
[22] H. Wang, "Signer-admissible strong designated verifier signature from bilinear pairings", Security and Communication Networks (7), Wiley, pp. 422–428, 2014.
[23] SK.-H. Islam, G.-P. Biswas, "Provably secure and pairing-based strong designated verifier signature scheme with message recovery", Arab Journal of Science Engineering (40), Springer, pp. 1069–1080, 2015.
[24] X. Hu, H. Xu, Y. Liu, J. Wang, W. Tan and X. Zhang, "An Efficient Designated Verifier Signature Scheme with Pairing-Free and Low Cost", Security and Communication Networks, 9(18), pp. 5724-–5732, 2017.
[25] X. Hu, W. Tan, H. Xu, J. Wang and Ch. Ma, "Strong Designated Verifier Signature Scheme with Undeniable Property and Their Application", Security and Communication Networks, pp. 1-–9, 2017.
[26] A.-U. Khan, B.-K. Ratha, "A Secure Strong Designated Verifier Signature Scheme", International Journal of Network Security, Vol.19, No.4, PP.599–604, 2017.
[27] Q. Huang, G. Yang, D. –S. Wong and W. Susilo, "Efficient Strong Designated Verifier Signature Scheme without Random Oracles or Delegatability", Cryptography eprint Archive Report 2009/518, http://eprint.iacr.org/2009/518.pdf.
[28] Y. Chen, Y. Zhao, H. Xiong and F. Yue, "A Certificateless Strong Designated Verifier Signature Scheme with Non-Delegatability", International Journal of Network Security, Vol 19(4), pp. 573–582, 2017.
[29] P. Rastegari, M. Berenjkoub, M. Dakhilalian, W. Susilo, "Universal designated verifier signature scheme with non-delegatability in the standard model", Information Sciences 479, pp. 321–334, 2019.
[30] Y. Zhang, Y. Zhang, Y. Li, et al., "Strong designated verifier signature scheme resisting replay attack", Information technology and control 44 (2), pp. 165–171, 2015.
[31] Ch. Li, S. Zhang, Y. Zhang and Y. Xie, "An improved strong designated verifier signature scheme", International Journal of Distributed Sensor Networks 14(12), pp. 1–7, 2018.
[32] S.-G. Worku, Ch. Xu and J. Zhao, "Cloud data auditing with designated verifier", Frontiers of Computer Science, 8(3), pp. 503–512, 2014.