IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

An Enterprise Rights Management System for On-the-field Maintenance Facilities

LUIGI CATUOGNO[1], CLEMENTE GALDI[1], and DANIEL RICCIO[2]

[1]L. Catuogno and C. Galdi are with Università di Salerno, Salerno, Italy. (e-mail: {lcatuogno,clgaldi}@unisa.it)

[2]D. Riccio is with Università di Napoli Federico II, and with Institute for High Performance Computing and Networking, CNR, Naples, Italy. (e-mail daniel.riccio@unina.it)

Corresponding author: C. Galdi (e-mail: clgaldi@unisa.it).

This research was partially supported by the ECSEL-JU under the program ECSEL-Innovation Actions-2018 (ECSEL-IA) for research project CPS4EU (ID-826276) research project in the area Cyber-Physical Systems.

ABSTRACT On-the-field maintenance of complex equipments, that may involve multiple subjects and stakeholders, is one of most challenging scenarios for Enterprise Rights Management (ERM). In this paper, we present an ERM system that guarantees the "on-site" protection of information confidentiality. In particular, our system features local data encryption and minimal data transfers. A secure key management protocol is executed by the devices operating on-site and the remote manufacturer's support center and guarantees an efficient and dynamic enforcement of arbitrary data-provider-defined access policies.
Operator identities are verified by means of strong multi-biometric verification schemes whilst protecting their biometries by means of cancelable biometries. To this end, we provide the first experimental evaluation of cancelable biometrics based on the fusion of face and voice biometries, that may be of independent interest.

INDEX TERMS Enterprise rights management, maintenance support systems, multi-biometric identification, cancelable biometrics.

I. INTRODUCTION

CYBER-PHYSICAL SYSTEMS (CPS) constitute a key enabler in innovation for the current economy. The availability of devices and networks with performance that where unthinkable only few years ago, makes possible the development of systems that provide innovative services at competitive costs. At the same time, the widespread diffusion of such systems poses new challenges in specific application contexts. Whenever CPS are used in critical scenarios where information security needs to be guaranteed at high levels, the presence of humans-in-the-loop may constitute a huge security threat that needs to be properly considered. On the other hand, in these contexts, one key issue is the seamless integration of human identification/authorization mechanisms with high-secure and flexible data protection and usage mechanisms. Indeed, a system that requires highly complex human identification procedures may become unusable. In this paper, we consider such scenarios and propose a secure solution that can be easily adapted to many contexts with similar security requirements.

In order to be concrete, we consider the following application scenario: Manufacturers of large and complex equipments such as industrial/military machinery or vehicles, provide their customers with several support maintenance services. These facilities involve several actors such as manufacturer's in-house experts who provide remote assistance, on-the-field intervention team (frequently outsourced to external contractors), and customer's trained personnel. Furthermore, maintenance contracts options may range from simple recurrent documentation update/upgrade to online expert assistance to on-the-field maintenance teams while they are operating. In a typical deployment of online assistance applications, the on-site team uses a camera for transferring live images from the intervention site to the remote assistance team. In this way, in-house experts have a clear idea of the issues to be solved, and they can provide effective and efficient assistance.

This online scenario is quite common and raises serious concerns regarding information security. Indeed, communication between the pool of experts and on-the-field operators, as well as the contents of any documentation or identification credential delivered during the intervention, carry a considerable amount of information regarding the product and the customer. Exposing such information to unauthorized parties may lead to the disclosure of manufacturer's industrial secrets or the infringement of secrecy policy the customer has to fulfil.

Enterprise Rights Management (ERM) aims at preserving the security of corporate private information throughout its whole lifecycle (even while flowing through different administrative and technological domains), ensuring the capability to enforce organizational access control policies regardless to the time and the place it is accessed.

In an ERM system, restricted contents (e.g., documents, e-mails, executive communications, notes...) are encrypted and linked to security "metadata" which carries its access control policy, encryption keys, etc. The metadata is stored by the data owner whereas the document is intended to be distributed within (and possibly beyond) the corporate boundaries. Each document request is associated to the corresponding metadata evaluation request that is delivered to the data owner. The system authenticates the requester, verifies whether the request is compliant with the access control policy stated for the document and eventually releases the decryption keys.

However, the on-the-field maintenance scenario we depicted above, remains one of most challenging for ERM. Indeed, security decisions could depend on environmental factors. Moreover, unforeseen conditions and events might make necessary to bypass or locally override the policies. In order to take into account these factors, ERM architectures leverage local trusted security agents which are in charge of gathering environmental information (e.g., through GPS) to be attached to the access request, and trustworthily enforce the policy decision, preventing misbehaving by the local operator. Furthermore, third-party operators' privacy should be clearly guaranteed in order to improve system acceptance.

In this paper we present an ERM system, specifically designed to support the maintenance operations in remote facilities which provide on-line assistance. We stress that, in these scenarios, the maintenance contract itself requires the existence of an online connection between the intervention site and a remote pool of experts. From this point of view, we study the problem of efficiently using such a feature for guaranteeing system's security. No assumption is made on documentation formats but we allows its oblivious navigation. Data release can be driven by fine grained context aware role-based access control policies. Device and operator trustworthiness can be enforced through third party equipments or infrastructures.

Operator authentication is based on non invasive multibiometric cancelable measurements. In order to improve system acceptance, user templates can be stored on a device owned by the operator. We provide the first experimental evaluation of cancelable biometrics based on the fusion of face and voice biometries. In particular, since it has already been shown in the literature that combining face and voice provides an accurate authentication protocol [44], our experiments are aimed at demonstrating that cancelable keys represent a valid tool to implement a challenge-response secure protocol. For this reason, we believe that even if limited in size, only 20 subjects, the corpus adopted for the experiments, can be considered acceptable for this purpose.

Beyond ERM, our infrastructure naturally fits different scenarios. For example, within e-Health applications, managing Electronic Health Records (EHR) raises similar issues. Indeed, EHRs are shared across different domains (e.g. public healthcare, social security, insurance companies, outsourced service providers) enjoying different access privileges.

We present the first challenge-response cancelable multibiometric authentication system that separates user credentials, stored on a personal-user device, from the measurement device that, in our context, is a third party one. The proposed system is able to interact with a remote data-owner site that is allowed to dynamically override device-driven access control policies. Our architecture is modelled upon the concept of Trusted Execution Environment (TEE) [25], which guarantees application and execution integrity. A preliminary version of this paper appeared as [14].

II. RELATED WORKS

ERM systems enforce access control over confidential documents throughout their whole lifecycle, within the boundaries of a corporation or within a business to business information flow. A number of solutions, e.g., [3], [34], addressing content protection within proprietary applications and file formats, have been proposed.

ERM systems prevent information leakage or document theft by both insiders and parties belonging to different domains who are authorized to cooperate on some sets of documents. For example, in [1], authorized personnel can transfer confidential documents only in encrypted form and only amongst authorized devices which are located within the corporate premises, regardless the transmission mean including both mobile storage and network. ERM-TVD [24], builds an ERM system on top of Trusted Virtual Domains (TVD) [9] and it is particularly suitable for multi-level corporate networked infrastructures.

File system level encryption is undoubtedly a fundamental component of every ERM system [30]. Cryptographic file systems feature transparent data encryption on top of a wide variety of storage devices (e.g., see [13], [16], [39]) where data is only stored in encrypted form. Authorized users access protected files by means of legacy applications, that are usually unaware of being accessing encrypted resources, as long as the proper encryption key is made available. In [6] file keys are released only if a certain number of file owners agree in reconstructing it through an interactive protocol. Shield [39] features a general purpose hierarchical key management and delivery for encrypted files stored in the cloud.

The widespread of mobile technologies and their application to ubiquitous computing is creating new possibilities and new challenges to the design of ERM systems [21].

Access control has been a long standing research topic in the field of computer security. Currently, a de facto standard for describing access control policies is Role Based Access Control [38], or RBAC for short. There exist a number of RBAC extensions that are particularly suitable for defining policies in the context of mobile and context aware systems, e.g. [4], [29], [31] just to name a few. Our system does not pose any constraint on the access control system and it is flexible to support any context aware access policy.

Despite plenty of attempts to enhance their security and reliability [17], old-fashioned password based schemes are no longer suitable for current application scenarios. Authentication “ergonomics” has been actively studied leveraging different technologies such as smart cards and crypto-token [43] or graphical passwords [10]–[12], [41].

Biometric verification systems aims at verifying the compatibility of a set of biometric measurements agains the ones that are present in a given template. Such systems work in consecutive steps: (a) feature extraction from the biometric measurements; (b) scoring the likelihood between extracted features and the user template and (c) decide whether or not measurements are close to the original template. Each biometric trait suffers specific weaknesses. It has been shown [2], [28] that verification systems that use multiple biometric traits or multi-factor schemes [27], [40] provide effective solutions for these type of problems. In multi-biometric systems, multiple decision pipelines need to converge to a unique decision (fusion). We focus on the fusion at the score level of face and voice biometries [22], [23]. It is known that current techniques that are used for voice and face classification cannot be used in isolation in an uncontrolled settings because of their sensitivity to signal distortions. However, in [44], the authors show that a multi-biometric system, jointly using voice and face recognition, can provide an effective solution in outdoor conditions. In order to provide user privacy [33], we guarantee the security of biometries by using cancelable biometrics. Most of the existing techniques implementing cancelable biometrics exploit non reversible transformations [35], which project real biometric data in a new space, while preserving the topological properties of the original feature space.

In our work, we focus on the online maintenance setting. A solution for an off-line variant of the problem has been presented in [15], where the authors describe an ERM system that adapts the biometric key binding scheme presented in [37] in order to provide a solution for a maintenance scenario with an off-line data owner.

III. SYSTEM OUTLINE AND REQUIREMENTS

A. APPLICATION SCENARIO

A manufacturer, also referred to as the Data Provider (DP), sells (or leases) industrial machineries along with a subscription to an on-line support service provided by an expert room. In this scenario, the online pool of experts communicates with the remote maintenance team by means of a video streaming of the maintenance site and a bidirectional audio streaming. The DP owns all the sensitive information delivered by the expert room (including e-mails, documents, etc.) while processing the support queries. Notice that, since such service requires an on-line support, the continuous availability of online experts is a requirement for our system.

Maintenance interventions are performed on-the-field, e.g., onboard a ship, by a team of operators, in a continuous online connection with the expert room. To this end, the DP provides the on-site team with trusted Company Devices (CD) that are used exclusively for the operations related to remote maintenance. The DP can store into the device memory part of the documentation in an encrypted form. On-site operators may access the documentation only if the DP-defined access policy allows to or if the experts deem it necessary. We stress that our system is flexible as it allows the data provider to define arbitrary release policies that can be even adapted while the operations are performed, e.g., [4].

On-the-field operators are registered to the DP authentication domain. A multi-biometric verification scheme is used to identify each operator. Our proposal fully exploit off-the-shelves cameras and microphones, currently available on commercial devices, for face and voice recognition. Each operator stores her own biometric data, in a standard X.509v3 certificate, along with her own public/private key pair on a her own device, which we refer to the User Device (UD). The UD is used to improve systems acceptance and user privacy since user credentials (a) are stored on a user-owned device and (b) never leave such device.

B. TRUSTED EXECUTION ENVIRONMENT

Our system implementation is based on the Trusted Execution Environment (TEE) technology [25]. TEE-enabled devices run two distinct execution environments, the Rich Execution Environment and the Trusted Execution Environment. The former is devoted to the execution of legacy OSes and applications (so called RichOS and Rich Apps or RA) and provides a normal security level; the latter runs a Trusted Operating System (TrustOS) which, in turn, takes care of guaranteeing applications’ integrity and the execution of Trusted Applications (TA) as isolated workloads. Furthermore, TEE provides each TA with a secure storage, typically used for keys, guaranteeing exclusive access to its own application data. Each trusted agent in our architecture is implemented as a TA. Notice thats TAs are, by assumption, trusted. This means that each TA does exactly what it is supposed to do. Notice that, the mere execution of software components within trusted isolated environments, does not guarantee the security of a system. Indeed, there exists stringent models and certification procedures [7], [18]–[20], [36] that have been defined to provide solid evidences of concrete system security that have to be applied even when secure containers are available. One key issue to solve, that is out of the scope of this paper, is the design of ad-hoc procedures, e.g., [8] for remotely updating/upgrading TAs. Due to space limitations, we refer interested reader to [25].

C. THREAT MODEL

We assume that the DP is trusted and performs all the required operations correctly. Since an online DP is a requirement, any fault of this component has to halt the service.

We consider attacks of insiders in which authorized users try to access information they are not allowed the current context, e.g., accessing file X in location Y when the access policy allows the access to X only in location Z.

Thus, an adversary has access to the CD and to the UD. Specifically, the adversary has full access to unprotected storage components and to unprotected volatile memory in the CD and UD. The goal of the attack is to get access to the information stored on the CD in a given context without having the required authorization.

This type of adversary can (a) legitimately authenticate using their own biometric credentials and measurements and (b) can monitor and store the content of unprotected memory and storage components of CD and UD.

Notice that, once the content of some data unit has been released by the system, we assume that the information is public. Nevertheless, the system should forbid the attacker to circumvent the access policy of previously-released data units. This translates in the impossibility for the attacker to obtain the encryption keys used by the system.

D. COMMUNICATION CHANNELS AND KEY MANAGEMENT

In the scenario depicted above, we assume the communication among the agents to occur as follows. The DP communicates exclusively with registered CDs and UDs. The communication between the UD and the DP occurs only through the CD the user is using. The digital certificates associated to each agent are used to create mutually authenticated DP-CD and CD-UD secure channels.

In our architecture, the CD and UD are required to feature a local "trusted agent" guaranteeing that local policy enforcement and keys/credentials management are trustworthily accomplished. This is to prevent that potential adversaries having stolen the device (or malicious insiders) exploit the CD and/or the UD, in order to obtain any key. In our system, the trusted agent obtains, stores and eventually deletes each encryption key every time the protocols require so. For this reason, the file key never leaves the "trusted agent" (whose memory is safe). Therefore, document browsing applications are designed to ask the trusted agent, to decrypt data units on demand.

E. DATA STORAGE

Users are provided with a UD featuring tamper-resistant technologies which carries personal and corporate-released certificates, user identifier, biometrics and digital keys and session identifiers.

The CD stores its device certificate, device identifiers, public/private keys and the DP certificate as well as, during the operations, the device securely stores and manages session handlers and keys. This device keeps track in a local CDDB of the encrypted data units it currently stores. It needs to associate, to each unit, its name, its content, some token containing the file key k, and the metadata associated to the file. Finally, our system requires that the CD is able to trustworthily enforce the access control policy over data units and encryption keys on behalf of the DP. In particular, it is required that the CD is able to deny the encryption keys to (no longer) unauthorized users.

The Data Provider holds three databases. The first one stores the digital certificates associated to the different registered entities. The second keeps track of the active sessions and stores the session id, the CD and UD ids and the session key. The last database, keeps track of the status of deployed CD. In other words, for each CD, the database stores the data unit name along with the random key used to encrypt it on the specific CD. Figure 1 shows the relationship among the different architecture components.

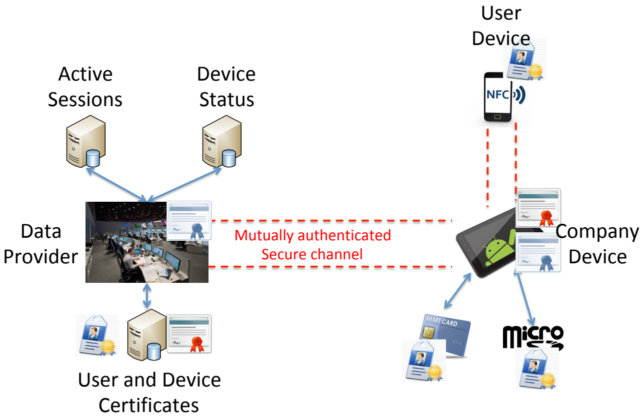

FIGURE 1: System architecture.

IV. CANCELABLE BIOMETRICS USING FACE AND VOICE

In this section we present the cancelable biometric authentication scheme based on face and voice measurements we use in the proposed system.

A. THE VERIFICATION SCHEME

The user is identified by a multi-biometric verification scheme that fuses face and voice at a score level. The biometric key held by the parties is obtained as follows: a face image and one-dimensional voice signal are processed separately, so obtaining two different features vectors, one for each biometric trait. Both feature vectors consist in a sequence of real numbers, whose length n may range between $[500, 10000]$. Thus, given a sequence of real numbers b, a cancelable biometric key b' could be obtained according to the Multispace Random Projections (MRP) [42] technique. The MRP method relies on the Johnson-Lindenstrauss lemma stating that is possible to embed any set of k points in n-dimensional Euclidean space into a low-dimensional space, while preserving the pairwise distance of any two points within an arbitrarily small factor. Considering that biometric keys are vectors of real values with a fixed size n, they can be though as points in n-dimensional Euclidean space and can be projected in a low dimension random subspace that alter the data original form but still preserves statistical characteristics. In other words, biometric keys that match/mismatch in the original n-dimensional space having distance lower/greater than the acceptance threshold of the system, still behave coherently after been projected in the random subspace, since statistical characteristics are preserved. This allows to setup a challenge-response verification protocol where a party, called the verifier is able to check wether the multi-biometric template she holds is consistent with the features measured by another party, the prober. At high level, the verifier sends a random challenge to the prover who sends back a function of the stored biometries and received challenge. The verifier checks wether the received value is consistent with the composition of the challenge with the biometries that she holds. In more details, the MRP algorithm generates a random matrix R of size $m \times n$ (where $m < n$) and computes a cancelable instance $b^{'}$ as $b^{'} = \sqrt{1/m}\ R\, b$. In the proposed verification protocol, the verifier generates a random matrix R of size $m \times n$ (where $m < n$), and sends R to the prover as a challenge. The prover computes a cancelable instance $b^{'}_{P_{face}}$ and $b^{'}_{P_{voice}}$ of its face and voice biometric keys $b_{P_{face}}$ and $b_{P_{voice}}$ and sends them back to verifier as a response to the received challenge. The verifier checks the response sent by the prover. In more details, it computes $b^{'}_{V_{face}} = \sqrt{1/m}\ R\, b_{V_{face}}$ and $b^{'}_{V_{voice}} = \sqrt{1/m}\ R\, b_{V_{voice}}$ and calculates the Euclidean distances $d(b^{'}_{P_{face}}, b^{'}_{V_{face}})$ and $d(b^{'}_{P_{voice}}, b^{'}_{V_{voice}})$, separately. The obtained real values are mapped into the range [0,1] and fused at score level according to a specific fusion rule (Simple Sum, Minimum, Product and Sum Product Rule). If the fused distance value is lower than a fixed threshold t_V, the verifier grants the user, otherwise it refuses the access. Notice that t_V is a system parameter that depends on biometric features used by the verification algorithm and it can be tuned during system setup, once and for all. We notice that the biometric keys on the CD are obtained by sampling the user biometrics using the device camera and microphone while the keys on the UD and DP are the ones stored in the user certificate.

B. EXPERIMENTAL EVALUATION

The aim of this section is to present the results of the different tests performed on the face/voice multi-biometric scheme adopted in the proposed framework. Face and voice both implement a processing pipeline that includes three modules: i) the correction of distortions in the input biometric sample, ii) the extraction of the biometric features vector, and iii) the projection of the feature vector into a randomly generated low dimensionality space (cancelable template). In more details, a Viola-Jonhes face detector [45] is adopted to locate the face ROI, which undergoes an Active Shape Model to detect 68 face markers (the center of the eyes, the corners of the nose, ...). In order to correct the pose distortion, the detected markers on the input face image are matched with their homologous in a reference frontal face model, so that the face image is frontalized by applying local affine transformations. The frontalized face is projected onto a submanifold of the face space generated by the Orthogonal Laplacianface (OLPP) [5]. Orthogonal Laplacianface preserves the metric structure of the face space, so the coefficients obtained by the OLPP approach provides a feature vector with high discriminating power. The feature vector is further projected onto a randomly generated low dimensional space by applying the Multispace Random Projections method, so to generate a cancelable biometric template. As regards the voice, speaker verification systems can be grouped in two classes: Text-Independent Speaker Verification (TI-SV) and Text-Dependent Speaker Verification (TD-SV). According to results presented in the literature, the former show the advantage of performing user verification without constraints on speech contents, but they require a long training and good utterance to guarantee good performance. The latter require the speaker pronouncing exactly the password the user has been enrolled with, but they show to be more robust in non ideal conditions. It comes clear that choosing a good password represents a crucial aspect for a TD-SV system. Among the possible several words of the Italian language we chose the word "alano" which is composed by the vowels "a" and "o" and sonorants "l" (alveolar lateral approximant) and "n" (nasal), so it provides distinctive biometric features. The voice module applies spectrum analysis to the input biometric sample and extracts MEL-frequency cepstrum coefficients (MFCCs) that are then rearranged into a feature vector. A cancelable biometric template for the voice is obtained by projecting the feature vector onto a randomly generated low dimensional space by applying the Multispace Random Projections method [42]. The proposed system implements a multi-biometric verification protocol, which combines face and voice at the score level. In other words, face and voice are processed separately and single scores are computed by comparing biometric templates according to a distance measure. In particular, the Euclidean distance has been adopted in our experiments. The face and voice scores are then normalized in the interval [0,1) and are combined by means of a fusion rule. It appears that score normalization and fusion represent the major aspects of a multi-biometric system. Indeed, the former plays an important role in the score fusion process, since face and voice matching generally produce real-valued scores with different distributions, which must be normalized into the range [0,1]. The latter is the core of the fusion operation, as it rules the combination of single scores to obtain a global numerical score. In [23], five techniques have been considered for the normalization of the score (Min-Max, Z-

Score, Median-MAD, Tanh and Modified Double-Sigmoid) and four rules have been investigated for score fusion (Simple Sum, Minimum , Product and Sum Product Rule). However, unlike the experimentation conducted in [23], we replaced the modified double-sigmoid with another improved version of the sigmoidal normalization function that is the quasi sigmoidal proposed in [32]. The proposed multi-biometric scheme also shows differences with the protocols proposed in [32], as it implements user verification instead of user recognition. This is a crucial aspect, since user verification performs a 1:1 match, so making the derivation of side information like the reliability index defined in [32] unfeasible. Moreover, the proposed system introduces an additional module to generate cancelable templates instead of directly matching feature vectors like in [32].

To the best of our knowledge, there are no existing multi-biometric database providing both face and text-dependent speech, so we considered chimeric users, where face comes from the SC-Face dataset [26] and voice is from a proprietary dataset. The number of subjects considered is 20, 10 women and 10 men, each with at least 3 face images and 3 voice recordings. The database is divided into two parts, called sessions, which differ from each other in the acquisition conditions, so to achieve a more complete assessment of the algorithm. The first session consists in two samples (face image/voice recording) per subject, while the second one contains one sample per subject. Sessions differs with respect to the quality of samples. Indeed, the first session, namely clean, includes face images of good quality and voice signals acquired in a recording studio, while the second session, namely noise, contains face images of low quality and voice signals recorded in a recording studio where it was introduced a source of noise, namely a playing radio.

In order to assess the performance of the proposed scheme, two experiments have been performed according to the closed universe model, meaning that every individual in the probe (identities to be verified) was also present in the gallery (identities enrolled into the system). Performances are measured in terms of Recognition Rate (RR), Equal Error Rate (EER), and Area Under Receiver Operating Characteristic (AUC) curve. In both experiments, face and voice biometric systems are first assessed separately, and then all possible combinations of score normalization and fusion techniques are considered as a multi-biometric scheme. In the first experiment, the first sample (face image/voice recording) in session clean is considered as the enrolment for each subject, that is the gallery consists of 20 biometric samples of good quality. The second acquisition in session clean is considered for testing, so the probe includes 20 biometric samples of good quality, that is one face image/voice recording per subject. The performance of single biometric systems is RR=0.85/EER=0.1461/AUC=0.870 and RR=0.95/EER=0.0513/AUC=0.985 for face and voice, respectively. The results of different multi-biometric schemes are reported in Table 1. In the second experiment, the gallery is the same considered for the first experiment, while the probe consists of 20 samples selected from session noise (one per subject). The performance of single biometric systems is RR=0.70/EER=0.2500/AUC=0.817 and RR=0.70/EER=0.1618/AUC=0.934 for face and voice, respectively, and results of different multi-biometric schemes are reported in Table 2. Results in Tables 1 and 2 show that the performance of the multi-biometric system is strongly influenced by the normalization function. In particular, according to findings of [32], it can be noticed that quasi-sigmoidal function provides the best performance in average. This can be attributed to the capability of quasi-sigmoidal function of better preserving the original score distribution while rescaling values in the [0,1) interval. As regards the combination rules, results highlights that for clean input samples both sum and product rules show a good performance. However, EER values in Table 2 point out product rule performs worse than sum rule, that is quite coherent with other results in literature. Indeed, it has been also demonstrated that sum rule is more robust with respect to noise. As it could be expected, the Sum Product Rule that represents such a kind of combination of the sum and product rule provides the best performance in average when original scores are normalized by the Quasi Sigmoidal function.

V. SYSTEM OPERATION

Our system's operations run through two phases: Registration and Execution.

The Registration phase is executed once for every involved device or agent and consists in identifying devices and operators and preloading on CDs and UDs the required digital certificates described in Section III-E.

The Execution phase is an actual "operational" phase, and it is executed before a maintenance operation starts. Whenever an operator requires the creation of a new session, the system uses the device certificates to create mutually authenticated secure channels among the actors. At this point, the system identifies the user using a multi-biometric verification scheme, which combines face and voice. Biometric samples are taken by using the device front camera and its microphone. A session key $\overline{K_s}$ is generated in a non-cooperative way by DP and CD. This key is computed as $\overline{K_s} = k_1 \oplus k_2$. In a first step DP sends k_1 to the UD and waits for its signature on k_1. The subkey k_2 is sent only after the signature is verified. This protocol ensures that the DP is indeed interacting with the legitimate owner of the user certificate stored on the UD. At the end of the Session setup protocol, the session key is signed by the UD and sent back to the DP as a proof of correct reconstruction.

The DP controls data release over different sessions as follows. Each DataUnit stored on a specific CD is encrypted using a random key, referred to as the file key. All file keys associated to a specific session are encrypted using a random session key. The deletion of the session key is sufficient to logically delete each file on the device as the file keys will become unavailable. Notice that, since CD is implemented by a TA, it actually removes keys whenever it is supposed to

TABLE 1: Results of the fusion scheme for probe samples selected from session clean

Normalization	Experiment II											
Method	Simple Sum			Minimum			Product			Sum Product		
	RR	ERR	AUC	RR	ERR	AUC	RR	ERR	AUC	RR	ERR	AUC
Min-Max	1.00	0.093	0.954	1.00	0.001	0.999	1.00	0.048	0.996	1.00	0.100	0.999
Z-score	1.00	0.100	0.961	1.00	0.000	1.000	0.85	0.151	0.879	0.10	0.490	1.00
Median-MAD	1.00	0.100	0.956	1.00	0.000	1.000	0.85	0.152	0.872	0.45	0.286	1.00
Tanh	1.00	0.063	0.968	1.00	0.007	0.986	1.00	0.063	0.968	1.00	0.100	0.986
Quasi Sigmoidal	1.00	0.040	0.998	0.95	0.001	0.999	1.00	0.001	1.000	1.00	0.006	0.999

TABLE 2: Results of the fusion scheme for probe samples selected from session clean

Normalization	Experiment II											
Method	Simple Sum			Minimum			Product			Sum Product		
	RR	ERR	AUC	RR	ERR	AUC	RR	ERR	AUC	RR	ERR	AUC
Min-Max	0.80	0.146	0.945	0.70	0.148	0.925	0.85	0.164	0.940	0.80	0.153	0.944
Z-score	0.80	0.150	0.950	0.70	0.147	0.934	0.50	0.248	0.854	0.05	0.667	0.293
Median-MAD	0.80	0.148	0.948	0.70	0.151	0.931	0.50	0.255	0.844	0.05	0.542	0.495
Tanh	0.80	0.147	0.920	0.70	0.163	0.919	0.80	0.147	0.887	0.80	0.149	0.949
Quasi Sigmoidal	0.85	0.098	0.959	0.70	0.191	0.928	0.80	0.105	0.956	0.80	0.100	0.958

do so. Whenever a new session is started, the DP generates a new session key that cannot be used to decrypt the file keys already stored on the device. When the user tries to access a data unit that is already stored (in an encrypted form) on the device, the access policy is evaluated. If the access is granted, the DP encrypts the file key associated to the data unit on the device under the new session key and sends it to the CD. If the data unit is not stored on the device, the DP will generate a random file key, encrypt the data unit using the file key and the file key under the current session key and transfer both to the CD.

This strategy clearly minimizes the communication overhead since in any case it is sufficient to transfer a single file key to enable the access to an entire data unit. Notice that the idea of sending on the same channel both an encrypted file along with the encryption key works because the channel used for the transfer is itself mutually authenticated and encrypted.

The proposed scheme works using the underlying assumption defined in Section III-D that once a given file has been accessed, its file key is securely deleted from the CD's memory. Similarly, whenever a session terminates, the session key is deleted from the memory. Notice that, in the simplest case, if the same user creates a new session and she has access to all the files she had requested before (e.g., in the case of static policies), the DP might simply resend the session key associated to the previous session. In a more dynamic context, even the same user might have access to a different set of data units, e.g., because the request occurs in a different location. In this case the DP will need to generate a new session key, and re-encrypt the file keys under the new session key. This apparent overhead has the advantage to provide the DP the possibility to fine-tune the access policy for each given context.

On the one hand this architecture creates a slight overhead for the DP as she needs to keep track of the state of each device. On the other hand this infrastructure has many advantages. Indeed it allows the DP to autonomously create the list of data units that are currently stored on every device and/or are currently readable in clear on a specific device. Furthermore, given the information stored by the DP, it is possible to enforce remote file removal policies by pushing random keys to the CD. Finally, and probably most importantly, it allows the DP to enforce dynamic and fine-grained access control policies since access to files are granted only after an explicit authorisation of the DP. In the following we describe the application protocols in the proposed system.

Operators identification: The CD acquires and computes the biometric key and acts as a prover for two independent executions of the protocol presented in Section IV-A; in the first one the UD acts as a verifier and the second one in which the DP acts as a verifier. At the end of this phase, both DP and UD have verified the identity of the operator using the template each of them stores against the measurements executed by the CD. Note that security and robustness of the identification protocol derives by observing that i) messages are exchanged only between parties registered by the DP, as defined in Section III-D; ii) the biometric template acquired for the user enrolment is not sent to the CD and it resides on the UD/DP; iii) CD performs the biometric measurements.

Session Key Setup: This protocol, described in Algorithm 1 in the Appendix, is run at the beginning of a new session and provides parties with a fresh and secure session key.

As a first step, the DP generates two subkeys k_1 and k_2, that will be used to generate the session key. The DP composes a message m_1 containing a session identifier, a random nonce, the timestamp and the subkey k_1. This message is signed and sent to the CD that forwards it to the UD. Once the signed message is received, the UD verifies the signature and checks that it has not received the same session identifier before. If all tests pass, the UD signs the received message and sends it back to the CD that forwards it to the DP. If the DP receives a valid reply to its previous message within a predefined time-bound Δ, it sends to the CD the subkey k_2 along with its signature on k_2. The CD verifies the signature and computes the session key $k = k_1 \oplus k_2$. At this point the CD deletes the subkeys k_1 and k_2 and sends to the DP the key k signed under its private key. In the last step the DP checks the received signature and verifies that the received key corresponds to $k_1 \oplus k_2$.

The confidentiality of the information exchanged is guaranteed by the fact that the messages are sent over a mutually authenticated, encrypted channel. Furthermore the signatures required by the protocol and its structure prevents key repudiation by the participating parties.

CD keys update: In our design, the session key is used to encrypt the file keys locally stored on the device. The session key setup procedure, described by Algorithm 2 in the Appendix, generates a new random session key for the new session. This new session key cannot be used to decrypt file keys since these are encrypted using a session key for a previous session. It is thus necessary to update the (encrypted) file key database. The update can be accomplished in two different ways. In an eager mode, the DP updates all the keys to which the user has access. Specifically, for each key currently stored on the CD, the DP evaluates the access policy associated to the data units it encrypts. If the access policy grants access to the specific data unit, the DP sends to the CD the file key encrypted under the new session key. In other words, for each data unit N, currently encrypted under the key k_N, and stored by the CD to which the current user is granted access by the DP access policy, the DP sends to the CD the encryption key k_N, encrypted under the current session key. In the lazy update, a file key is updated only when the corresponding data unit is requested.

File Request: The procedure, described by Algorithm 3 in the Appendix, is started by the CD that requires the specific data unit to the DP. Specifically, the CD sends to the DP a request containing the user identifier, the CD identifier and the data unit identifier N. Once it receives the request, the DP first verifies that the device and the user identifiers correspond to the ones associated to the current session and rejects the request otherwise. Subsequently, the access policy is evaluated. If the access is granted, the DP verifies whether or not the requested data unit has been already sent to the same device in a previous session. In the former case, the DP recovers the file key k under which the data unit has been encrypted on the requesting device, encrypts k under the session key and sends the encrypted key to the CD. In the latter case, the DP generates a new random file key k, and encrypts the requested data unit under k. The file key is then encrypted under the session key. The encrypted file key and the encrypted data unit are transferred to the CD. Finally, both the DP and the CD update their local databases.

File Access: The information currently stored on the CD are accessible exclusively by means of the current session key. For each file stored in the CD there exists a record in the CDDB that contains the corresponding file key encrypted using the current session key. Thus, the encrypted files on the CD can be partitioned into the ones that are accessible in clear in the current session and the ones that are not accessible.

Notice that data/page unit names or metadata might reveal by themselves sensitive information, e.g., a specific device is onboard a specific ship. A security extension to our system might require the encryption of metadata associated with the files, including the file name. Whenever the reference to a given data/page unit is encrypted, the actual file access must be preceded by a search within the CDDB.

VI. CONCLUSIONS

In this paper we have described an ERM system, specifically designed to support sensitive document management in remote maintenance operations with multiple stakeholders. Our ERM system provides the data owner full and dynamic control on the document release policy. A secure multi-biometric authentication scheme is used to identify operators whilst guaranteeing system usability and users privacy. Finally we have experimentally demonstrated the composability of the MRP technique with multi-biometry authentication based on face and voice recognition. Our architecture naturally fits other application scenarios with similar security requirements such as e-Health and homeland security.

REFERENCES

[1] Imad M Abbadi and Muntaha Alawneh. Preventing insider information leakage for enterprises. In Second Intl. Conf. on Emerging Security Information, Systems and Technologies (SECURWARE'08)., pages 99–106. IEEE, 2008.

[2] M. C. D. C. Abreu and M. Fairhurst. Analyzing the benefits of a novel multiagent approach in a multimodal biometrics identification task. IEEE Systems Journal, 3(4):410–417, Dec 2009.

[3] Adobe Systems. Adobe livecycle es4. http://www.adobe.com/products/livecycle.html.

[4] Piero A. Bonatti, Clemente Galdi, and Davide Torres. Event-driven RBAC. Journal of Computer Security, 23(6):709–757, 2015.

[5] Deng Cai, Xiaofei He, Jiawei Han, and H-J Zhang. Orthogonal laplacianfaces for face recognition. IEEE transactions on image processing, 15(11):3608–3614, 2006.

[6] A. Castiglione, L. Catuogno, A. Del Sorbo, U. Fiore, and F. Palmieri. A secure file sharing service for distributed computing environments. Journal of Supercomputing, 67(3):691–710, 2014.

[7] L. Catuogno and C. Galdi. On the evaluation of security properties of containerized systems. In 2016 15th International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security (IUCC-CSS), pages 69–76, Dec 2016.

[8] L. Catuogno, C. Galdi, and G. Persiano. Secure dependency enforcement in package management systems. IEEE Transactions on Dependable and Secure Computing, pages 1–1, 2017.

[9] Luigi Catuogno, Alexandra Dmitrienko, Konrad Eriksson, Dirk Kuhlmann, Gianluca Ramunno, Ahmad-Reza Sadeghi, Steffen Schulz, Matthias Schunter, Marcel Winandy, and Jing Zhan. Trusted virtual domains–design, implementation and lessons learned. In Trusted Systems, pages 156–179. Springer, 2009.

[10] Luigi Catuogno and Clemente Galdi. A graphical PIN authentication mechanism with applications to smart cards and low-cost devices. In Proc. of 2nd Intl. Workshop on Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks (WISTP), pages 16–35, 2008.

[11] Luigi Catuogno and Clemente Galdi. Analysis of a two-factor graphical password scheme. Int. Journal of Information Security, 13(5):421–437, 2014.

[12] Luigi Catuogno and Clemente Galdi. On user authentication by means of video events recognition. J. Ambient Intelligence and Humanized Computing, 5(6):909–918, 2014.

[13] Luigi Catuogno and Clemente Galdi. A fine-grained general purpose secure storage facility for trusted execution environment. In Proceedings of the 5th International Conference on Information Systems Security and Privacy, ICISSP 2019., pages 588–595, 2019.

[14] Luigi Catuogno, Clemente Galdi, and Daniel Riccio. Flexible and robust enterprise right management. In IEEE Symposium on Computers and Communication, ISCC 2016, Messina, Italy, June 27-30, 2016, pages 1257–1262, 2016.

[15] Luigi Catuogno, Clemente Galdi, and Daniel Riccio. Off-line enterprise rights management leveraging biometric key binding and secure hardware. J. Ambient Intelligence and Humanized Computing, 10(7):2883–2894, 2019.

[16] Luigi Catuogno, Hans Löhr, Marcel Winandy, and Ahmad-Reza Sadeghi. A trusted versioning file system for passive mobile storage devices. Journal of Network and Computer Applications, 38:65–75, 2014.

[17] Angelo Ciaramella, Paolo D'Arco, Alfredo De Santis, Clemente Galdi, and Roberto Tagliaferri. Neural network techniques for proactive password checking. IEEE Trans. on Dependable and Secure Computing, 3(4):327–339, 2006.

[18] Common Criteria Sponsoring Organizations. Common criteria for information technology security evaluation part 1: Introduction and general model, version 3.1 rev 4,, September 2012.

[19] Common Criteria Sponsoring Organizations. Common criteria for information technology security evaluation part 2: Security functional components, version 3.1 rev 4, September 2012.

[20] Common Criteria Sponsoring Organizations. Common criteria for information technology security evaluation part 3: Security assurance components, version 3.1 rev 4, September 2012.

[21] A.K. Das, D. Mishra, and S. Mukhopadhyay. An anonymous and secure biometric-based enterprise digital rights management system for mobile environment. Security and Communication Networks, 2015.

[22] M. Farrús, A. Garde, P. Ejarque, J. Luque, and J. Hernando. On the fusion of prosody, voice spectrum and face features for multimodal person verification. In International Conference on Spoken Language Processing (ICSLP), pages 1–4, 2006.

[23] Y. M. Fouda. Fusion of face and voice: An improvement. International Journal of Computer Science and Network Security, 12(4):37–43, 2012.

[24] Yacine Gasmi, Ahmad-Reza Sadeghi, Patrick Stewin, Martin Unger, Marcel Winandy, Rani Husseiki, and Christian Stüble. Flexible and secure enterprise rights management based on trusted virtual domains. In Proceedings of the 3rd ACM workshop on Scalable trusted computing, pages 71–80. ACM, 2008.

[25] GlobalPlatform. TEE system architecture v1.0. http://www.globalplatform.org, 2011. Last visited: Jan. 9, 2018.

[26] Mislav Grgic, Kresimir Delac, and Sonja Grgic. Scface - surveillance cameras face database. Multimedia Tools and Applications Journal, 51(3):863–879, 2011.

[27] D. He and D. Wang. Robust biometrics-based authentication scheme for multiserver environment. IEEE Systems Journal, 9(3):816–823, Sept 2015.

[28] A. K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1):4–20, Jan 2004.

[29] Michael S. Kirkpatrick and Elisa Bertino. Enforcing spatial constraints for mobile RBAC systems. In Proc. of the 15th ACM Symp. on Access Control Models and Technologies (SACMAT), pages 99–108, 2010.

[30] Sangho Lee, Hay-Rim Lee, Seungkwang Lee, and Jong Kim. Drmfs: A file system layer for transparent access semantics of drm-protected contents. Journal of Systems and Software, 85(5):1058 – 1066, 2012.

[31] Fei Li, Yogachandran Rahulamathavan, Mauro Conti, and Muttukrishnan Rajarajan. Robust access control framework for mobile cloud computing network. Computer Communications, 68:61–72, 2015.

[32] Maria De Marsico, Michele Nappi, Daniel Riccio, and Genoveffa Tortora. Nabs: Novel approaches for biometric systems. IEEE Transactions on Systems Man and Cybernetics - Part C: Applications and Reviews, 41(4):481–493, 2011.

[33] K. Martin, H. Lu, F. M. Bui, K. N. Plataniotis, and D. Hatzinakos. A biometric encryption system for the self-exclusion scenario of face recognition. IEEE Systems Journal, 3(4):440–450, Dec 2009.

[34] Microsoft Corporation. Microsoft rights management services. https://technet.microsoft.com/en-us/dn175750.

[35] Christian Rathgeb and Andreas Uhl. A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security, 2011(1):1–25, 2011.

[36] Elena Reshetova, Janne Karhunen, Thomas Nyman, and N. Asokan. Security of os-level virtualization technologies. In Karin Bernsmed and Simone Fischer-Hübner, editors, Secure IT Systems - 19th Nordic Conference, NordSec 2014, Tromsø, Norway, October 15-17, 2014, Proceedings, volume 8788 of Lecture Notes in Computer Science, pages 77–93. Springer, 2014.

[37] Daniel Riccio, Clemente Galdi, and Rita Manzo. Biometric/cryptographic keys binding based on function minimization. In 12th International Conference on Signal-Image Technology & Internet-Based Systems, SITIS 2016, pages 144–150, 2016.

[38] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. Role-based access control models. Computer, 29(2):38–47, 1996.

[39] Jiwu Shu, Zhirong Shen, and Wei Xue. Shield: A stackable secure storage system for file sharing in public storage. Journal of Parallel and Distributed Computing, 74(9):2872 – 2883, 2014.

[40] M. Sultana, P. P. Paul, and M. L. Gavrilova. Social behavioral information fusion in multimodal biometrics. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 48(12):2176–2187, Dec 2018.

[41] Xiaoyuan Suo, Ying Zhu, and G. Scott Owen. Graphical passwords: a survey. In Proceedings of 21st Annual Computer Security Application Conference (ACSAC), pages 463–472, 2005.

[42] A. Teoh and Chong Tze Yuang. Cancelable biometrics realization with multispace random projections. IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, 37(5):1096–1106, Oct 2007.

[43] J. L. Tsai and N. W. Lo. A privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE Systems Journal, 9(3):805–815, Sept 2015.

[44] H. Vajaria, T. Islam, P. Mohanty, S. Sarkar, R. Sankar, and R. Kasturi. Evaluation and analysis of a face and voice outdoor multi-biometric system. Pattern Recognition Letters, 28(12):1572–1580, 2007.

[45] Paul Viola and Michael Jones. Rapid object detection using a boosted cascade of simple features. In Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on, volume 1, pages I–I. IEEE, 2001.

APPENDIX. PROTOCOL SPECIFICATIONS

Each data unit is identified by a name N and its content by $C(N)$. We write $A \rightarrow B : m$ whenever an agent A sends a message m to an agent B. We will denote by $E_k(x)$ symmetric encryption/decryption of the plaintext x under the key k; Do to space limitations, we only report the formal specification of the session key setup protocol.

LUIGI CATUOGNO is network administrator at the Department of Computer Science of the University of Salerno, where he got his Laurea degree (M.Sc. equivalent) in 1999, his PhD in Computer Science in 2004 and a post-doc fellowship in 2009. He has been visiting student at New York University in 2002 and research assistant at Ruhr University of Bochum (Germany) in 2009. His research focuses on system security and privacy enhancing technologies.

CLEMENTE GALDI got a Laurea cum laude and PhD in Computer Science from Università degli Studi di Salerno in 1997 and 2002. He has been visiting researcher at Telcordia Technologies and DIMACS, New Jersey, USA. He has been post-doctoral fellow at Computer Technology Institute and University of Patras (Greece) (2001-2004), at Università di Salerno (2004-2006), Assistant Professor at University of Naples, Federico II (2006-2018). He is Assistant Professor at the Università di Salerno. His fields of interests are Data Security, Cryptography and Algorithm Design.

Algorithm 1: Session Key Setup

```
Parameter: $\Delta$ - Max delay
Output   : A session key $\hat{k_s}$ shared by CD and DP.
CD→ DP: $(Id_{CD}, Id_{UD}, \textit{New Session})$
DP:
    $Id_s \leftarrow unique\_identifier()$
    $r_s \leftarrow random\_nonce()$
    $k_1, k_2 \leftarrow random\_subkeys()$
    $t_s \leftarrow timestamp()$
    $m_1 \leftarrow (Id_s, r_s, k_1, t_s)$
    $\sigma_1 \leftarrow Sign_{DP}(m_1)$
DP→ CD→UD: $(m_1, \sigma_1)$
UD:
    if ($\textit{Verify}_{DP}(m_1, \sigma_1) \wedge ((Id_s, r_s) \notin \textit{UDDB}) \wedge (t_s - \textit{currentTime}() < \Delta)$) then
        $\sigma_2 \leftarrow Sign_{UD}(m_1)$
        Add $(Id_s, r, t_s)$ to UDDB
    else
        $\sigma_2 \leftarrow Reject$
    end
UD→CD→DP: $\sigma_2$
DP:
    if ($\textit{Verify}_{UD}(m_1, \sigma_2) \wedge (t_s - \textit{currentTime}() < \Delta)$) then
        $DP \rightarrow CD : (k_2, \sigma_3 = Sign_{DP}(k_2))$
        $\hat{k_s} \leftarrow k_1 \oplus k_2$
        Add $(Id_s, Id_{CD}, Id_{UD}, \hat{k_s})$ to DP_SESSION.
    else
        Reject
    end
CD:
    if $\textit{Receive}\ (k_2, \sigma_3) \wedge \textit{Verify}_{DP}(k_2, \sigma_3)$ then
        $\hat{k_s} = k_1 \oplus k_2$
        Secure_Delete($k_1, k_2$)
        $\sigma_4 = Sign_{CD}(\hat{k_s})$
        CD→ DP:$\sigma_4$
        Save $(Id_s, \hat{k_s})$ to Securely Deletable Storage
    else
        Reject
    end
DP:
    if $\textit{not}(\textit{Verify}_{UD}(\hat{k_s}, \sigma_4))$ then
        Delete
        $(Id_s, Id_{CD}, Id_{UD}, \hat{k_s})$ from DP_SESSION
        Reject
    end
```

Algorithm 2: CDDB Update

```
Input : DP: $\hat{k_s}, Id_s, Id_{CD}, Id_{UD}$
        CD: $\hat{k_s}$
DP:
    Extract $(Id_s, \hat{Id_{CD}}, \hat{Id_{UD}}, \hat{k_s})$ from DP_SESSION
    if $(Id_{CD} \neq \hat{Id_{CD}}) \vee (Id_{UD} \neq \hat{Id_{UD}})$ then
        Reject
    else
        foreach $(Id_{CD}, N, k_N)$ in DP_FILE do
            if $(AccessPolicy(Id_s, Id_{CD}, Id_u, N) = GRANT\_ACCESS)$ then
                $DP \rightarrow CD : (N, E_{\hat{k_s}}(k_N))$
            end
        end
    end
CD:
    foreach Received $(N, E_{\hat{k_s}}(k_N))$ do
        Replace $(N, E_{k_s}(k_N))$ with $(N, E_{\hat{k_s}}(k))$ in CDDB
    end
```

Algorithm 3: File Request

```
$CD \rightarrow DP : (Id_s, Id_{CD}, Id_{UD}, N)$
DP:
    Extract $(Id_s, \hat{Id_{CD}}, \hat{Id_{UD}}, \hat{k_s})$ from DP_SESSION
    if $(Id_{CD} \neq \hat{Id_{CD}}) \vee (Id_{UD} \neq \hat{Id_{UD}})$ then
        Reject
    else
        if $(AccessPolicy(Id_s, Id_{CD}, Id_{UD}, N) = GRANT\_ACCESS)$ then
            Extract $(Id_{CD}, N, k_N)$ from DP_FILE
            if Success then
                $DP \rightarrow CD : (N, E_{\hat{k_s}}(k_N))$
            else
                Generate random $k$
                Add $(Id_{CD}, N, k)$ to DP_FILE
                $DP \rightarrow CD : (N, E_{\hat{k_s}}(k), E_k(C(N)))$
            end
        else
            $DP \rightarrow CD$ : Reject
        end
    end
CD:
    if Receive $(N, EK[, EC])$ then
        Add $(N, EK[, EC])$ to CDDB
    else
        Reject
    end
```

DANIEL RICCIO received the Laurea degree (cum laude) and the Ph.D. in computer science from the University of Salerno in 2002 and 2006, respectively. He is currently an Associate Professor at the University of Naples, Federico II. His research interests include biometrics, medical imaging, image processing and indexing. He is also an Associate Researcher at the CNR-ICAR (Naples), where he is involved in the research activities of the Cognitive System Laboratory. Prof. Riccio is a member of IEEE since 2012 and of the Group of Italian Researchers in Pattern Recognition since 2004.

• • •