Dynamic Multiparty Authentication using Cryptographic Hardware for the Internet of Things

Hussain Al-Aqrabi, Anju P. Johnson, Richard Hill
Centre for Industrial Analytics
University of Huddersfield
Huddersfield, HD1 3DH, UK
Email: {h.al-aqrabi,a.johnson,r.hill}@hud.ac.uk

***Abstract*—The rapid development of various emerging technologies such as cloud computing and the Internet of Things (IoT) presents significant security and privacy challenges. In particular, complex and challenging applications involving various business parties have the requirement to delegate access control mechanisms securely to one or more parties, who in turn can govern methods that enable multiple other parties to be authenticated in relation to the services that they wish to consume. Moreover, modern integrated design and manufacturing follows a business model where different third-party vendors provide hardware, software, and manufacturing services, making it hard to ensure the trustworthiness of the entire process. The emergence of IoT has led to our use of Field Programmable Gate Array (FPGA) devices with Dynamic Partial Reconfiguration (DPR) abilities, which allows for modifications to the hardware implemented to undergo changes and incorporate dynamic addition/deletion of access using security protocols. We use, Physically Unclonable Functions (PUF), cryptographic hardware primitive which are based on a physical system having easy to evaluate, hard to predict and manufacturer resistant properties in developing a security protocol. In this paper, we combine the concepts of hardware security through PUFs and hardware evolution through DPR in providing dynamic secure multiparty authentication system.**

***Keywords*—** cryptographic protocol, dynamic partial reconfiguration, physically unclonable functions, cloud computing, analytics, security, multiparty interactions, Internet of Things

I. Introduction

The Internet of Things (IoT) refers to uniquely identifiable devices/objects connected to the internet that can sense data and react with their environment [1], [2]. Computing is focused on the vast amount of data collected and made accessible by connecting all smart objects within an IoT system [3]. IoT 'things' are dynamic in nature requiring flexible software and hardware [4]. Software applications are well known for their flexibility, but *plasticity* in hardware is an emerging field. The concept of flexible hardware was introduced with the advent of new technologies such as Dynamic Partial Reconfiguration (DPR) in re-programmable hardware such as Field Programmable Gate Array (FPGA) devices [5]. DPR enables the use of fewer or smaller devices, reducing power consumption and enhancing system upgrades. These features led to the growing demand for deployment of FPGAs in areas including IoT [6]. As software provides a very high amount of flexibility, which is lacking in hardware, FPGAs are thought to bridge this gap. However, the design of these systems can be challenging, and this is particularly true of the configuration controller. Currently, new tools have been widely developed to support and promote DPR capabilities in FPGAs [7].

Another highly demanding requirement for IoT is security [6], [8]. Nowadays cryptography has become part of our everyday lives due to the security requirement of more common activities including communication, encryption disks, and electronic money systems. Currently, hardware security, where programmable logic solutions can provide additional security in the form of cryptographic hardware solutions (CHS) are widely in research [9], [10]. Currently, most industrial sectors use hardware security modules (HSMs) to provide dedicated cryptographic services to ensure ultimate device protection with a dual focus on high performance and security [11]. Hardened authentications are highly resistant to remote attacks and are capable to meet any level of endpoint security and are high potential candidates for the future business. CHS in the form of Physically Unclonable Function (PUF) technology is world leaders in security IP cores [12]. Currently, IoT employs reconfigurable and lightweight devices with embedded security for a variety of applications [13], [14].

In a distributed system architecture such as cloud [15], the user becomes dynamic or system may need to upgrade their product to stay updated. As FPGAs are designed to provide the necessary flexibility due to the infield reconfigurable device features within limited time, they provide benefits to enterprises [16]–[18]. FPGAs are also increasingly used in embedded security applications as they provide flexibility including algorithm agility, architecture efficiency, resource efficiency, algorithm modification, throughput and cost efficiency [19]. All protection mechanisms in hardware-enforced using cryptographic techniques and dynamism using reconfiguration provide a compact solution for flexibility and security. It is also known that the use of programmable hardware in system implementation can improve performance. Although the relatively higher power dissipation of FPGAs in previous generations was a challenge to limit their deployment in power sensitive applications, Ultra low power FPGAs are now widely available for IoT usage. For distributed systems and IoT applications, DPR-enabled FPGAs are the platform of choice [6]. Furthermore, It may be subject to malicious circuit alterations, usually referred to as Hardware Trojan insertion [20], [21]. Such attacks use the same DPR capabilities that are otherwise so valuable. Therefore, proper defense strategies must be put in place to counter such threats while taking into account the inherent physical restraints of IoT. With the growing popularity of services delivered by cloud computing, it is important that both cloud providers and cloud users have confidence that there are appropriate safeguards in place to ensure an acceptable level of security and privacy mechanisms [22]–[24]. A number of researchers have contributed to strengthen security and privacy protection in cloud applications, and there are various cryptographic algorithms to address potential security and privacy problems in cloud [25]–[28]. It follows that research topics related to cloud security have attracted tremendous research interest [29]–[32].

The remaining part of the paper is organised as following. In section II, we discuss the multiparty delivery system emphasising security. Section III, describes the challenges associated with the design of multiparty system. Various multiparty authentication methods are provided in Section IV. In section V we describe the hardware security primitive used in this work. The proposed protocol for multiparty authentication is described in Section VI. Finally, we conclude the work with directions for future development in Section VIII.

II. Multiparty service delivery and security

As enterprises are being more conscious of data collection, analysis, modelling, and prediction, the need for systems with a faithful representation of business processes is becoming widespread. This means that the underlying digital services must demonstrate both robustness and flexibility to tolerate new and unanticipated business scenarios. As such, process flows may be difficult to predict in some instances, especially if a business offers bespoke services or products to customers, where a transaction may execute only once [33]. As a consequence of this, the eventual application that is delivered is underpinned by a collection of disparate services that are orchestrated at run-time, that may have origins in organisations that are heterogeneous. Each of the host organisations will have adopted security measures that are unique to the enterprise, with the effect that an application composed of multiple services will thus present a number of different security realms. Each realm typically consists of data that represents a collection of resource principals, that are registered with a trusted principal such as a certificate authority. The principals are governed by a set of security policies that control access to other services and resources within the scope of the application [34]. The certificate authority is deemed to be trustworthy across the application domain and is present to validate users and functions [35]. It is essential that each security realm is authenticated against to ensure that a principal has the appropriate security privileges to consume services marshalled by a security realm. The identity of a principal needs to be confirmed by the correct authentication process of the relevant realm so as to correctly identify and establish who the principal is. During the authentication process, security credentials that were given to the principal by the relevant security realm are used to authenticate it.

In the case of more complex application architectures, such as cloud-based services provision, each cloud may hide multiple instances of other clouds and/or services [36]. It follows that not only will there be numerous authentication mechanisms to keep maintained, but they will have to be invoked dynamically at run-time on demand. If separate authentication processes are established across disparate security realms, there is a potential for a significant increase in authentication workload and the consequential side-effects on network bandwidth and computational cycles [37]. The scenario where a multiparty session is composed of many two-party sessions is explored by in [38], which demonstrates that there is a need for a protocol for multiparty session authentication. There is an inherent challenge here that it is not always possible for a session participant to establish whether another session participant is actually a member of the multiparty session in progress.

III. Key challenges for multiparty environments

The wider distribution of of IoT nodes and the extent and nature of the data collected and transformed by IoT devices are a major challenge for security. The wider distribution of of IoT nodes and the extent and nature of the data collected and transformed by IoT devices are a major challenge for security. In the IoT domain, authentication permits the integration of various IoT devices deployed in various contexts. In view of the fact that services and organisations can adopt a collaborative process in an extremely vibrant and flexible manner, direct cross-realm authentication relationship is not simply a means of joining the two collaborating realms. The lack of authentication path connecting two security realms will necessitate two security realms, when working together, to follow a more traditional and long route that will involve creating a mutual trust entailing entering into contractual agreements, multi-round cooperation and human intervention.

The primary reason for this lack of progress is due to serious concerns about the security, privacy, and reliability of these systems. IoT is capable of monitoring all aspect of day-to-to life, including the above-mentioned concerns [39], [40]. Citizens, therefore, have legitimate concerns about privacy. In addition, businesses are concerned with damage to their reputations due to data being handled by wrong hands, and the governments fear the consequences of security risks [41]. Multiparty authentication is a complex challenge in a multi-cloud environment. These challenges increase in complexity when we consider the potential proliferation of devices in IoT systems. In general, such systems may be a one-to-one mapping between system access devices and the clouds themselves.

However, there are also several additional complications of numerous devices with varying degrees of functionality and capability. An example of such a device is a Wireless Sensor Network (WSN), which are often adaptive entities that may be applicable to the addition or removal of sensor nodes during operation.

Various reports predict a remarkable increase in the number of connected intelligent 'things' exceeding 20 billion by 2020 [42]. As we see the exponential growth of the connected devices, the predictions seem to be believable. If these predictions come true, then the demand for authentication of devices will be a major challenge to address, especially as there will be insufficient capacity to manually authenticate even a fraction of the devices and consequently, some automation will be mandatory.

A fundamental challenge in a complex environment like the IoT or multi-clouds is the necessity to manage and ensure communications that enable the required authentication approvals [43].

The use of Single Sign On (SSO) also allows the use of a key exchange technique to actually manage the provision of authentication credentials certified by a named authority. In addition, it eliminates the need for users to enter different security credentials multiple times [44], [45].

However, despite the relative simplicity of the technique, it simply provides a secure method of key exchange is insufficient for the situation when we need multiple parties to be capable to establish certain trust each other in a dynamic, heterogeneous environment, and therefore SSO technique is lacking in this regard.

IV. Authenticating multiple parties

With the explosive growth of Internet of Things applications the transition of traditional communication services to the Internet is becoming increasingly important for group communication. Several new online services and applications are emerging, such as Cloud computing which enables users to elastically scale their applications, software platforms and hardware infrastructures. These cloud implementations increase the sharing of resources by separating solutions into different tiers [46].

In contrast, where cloud computing systems share a domain, services for the delivery of data analytics are more prone to external threats such as: distributed attacks, malware attacks, and other known security and privacy issues for cloud computing [47], which are applicable to distributed systems also. Consequently, the growing proliferation of services offered by IoT technologies poses many risks related with security and privacy as well.

A. Dynamic authentication

In a multi-tenancy environment, Cloud-based business systems are dynamic and involve similarly dynamic authentication interactions. Hence, the authentication frameworks cannot be static. Burrows [48] proposed a tenant privacy framework using a global authentication register as an attempt to facilitate dynamic authentication.

Dynamic authentication creates a per-session authenticator using cryptography. With each authentication session between the requester and the verifier, a dynamic authenticator changes.

In order to obtain the registration application certificate, the register holds a private key and personal data for each tenant, and subsequently provides the requisite private key, providing that the personal data received by the system registrar is correct. Chen [49] posits that a multi-tenant database hosted on a cloud platform can serve the purpose of registering global authentication requests and transactions, to include the specific details of which stakeholder has initiated which transaction.

Each tenant is represented within the cloud service provider by way of a record of specific data, that is appended to existing tenant metadata.

It is the augmentation of this tenant data that enables the verification of private data that has been supplied previously, a scheme that was introduced by Pippa [50] and is described as identity-based cryptography. This approach ensures that tenants within a multi-tenant environment can only be granted access to the workspace that they have been allocated.

The root key (common for the entire cloud) is the public key that unlocks a cloud or grid-based workspace assigned to all valid cloud tenants.

Interaction between the client and server enables data regarding the client's identity to be exchanged for the purposes of verification. As part of this exchange, the public (root) key is included and added to the private key that was generated as a by-product of the interaction.

The authentication registry server uses the signature to add private key fields to the root key, for them to be sent to the client who has made the rquest. Furthermore, other server arrays, which are most likely to be clouds, can be allocated to undertake privacy-as-a-service duties. These duties include the ability to provide identity-based cryptography and identity-based signature generation for cloud computing [50]. Such clouds arrange the key structures as hierarchies as per Figure 1.

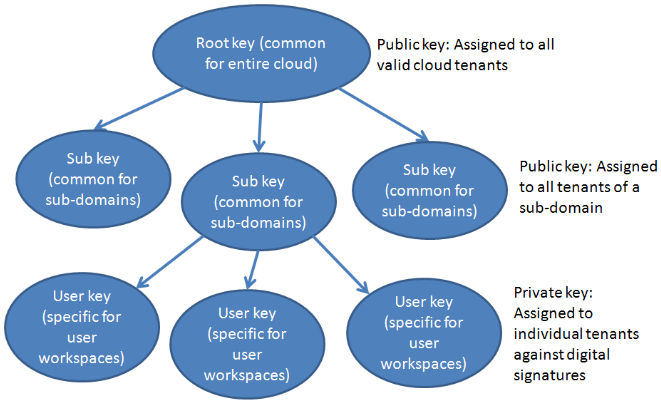
Root key (common for entire cloud)
Public key: Assigned to all valid cloud tenants
Sub key (common for sub-domains)
Sub key (common for sub-domains)
Sub key (common for sub-domains)
Public key: Assigned to all tenants of a sub-domain
User key (specific for user workspaces)
User key (specific for user workspaces)
User key (specific for user workspaces)
Private key: Assigned to individual tenants against digital signatures

Fig. 1. Hierarchical key structures in cloud computing [34].

Each key is composed of two sub-components. The first is a public key that is common across all authorised tenants of a cloud. The second component is a private key that is used by the tenants of a cloud sub-domain. This private key is generated as a by-product of a tenant's individual digital signature via a distinct cloud array.

B. Cloud sub-domains

Sub-domains within clouds are collections of virtual workspaces that are private to a set of tenants or a business organisation. Users who are not authorised are prevented from entering the workspaces by the use of public keys [51].

The granting of a public key is marshalled by a requirement to refer to personal records, such as employee data for instance. This is augmented by additional security from a private key that is issued to tenants, again using an suthorisation mechanism that depends upon the provision of information that is personal and can uniquely identify and distinguish a particular tenant.

It is the organisation that owns the private data (employee data in this example), that administers and hosts the private key component of the overall access key. The remaining component is the key to the sub-domain that is generated and managed by the cloud provider. This establishes a hierarchical organisation of the various key components, as illustrated in Figure 2, where a commonplace use case of a staff member needing to access operations data from a remote cloud.

C. Federation across clouds

As the number of parties requiring authorised access increases, so does the complexity of the interactions that need to be managed via the home cloud. Agent-based federation of services across multiple clouds [52] is one solution to the challenge, which simplifies the complexity by defining roles to manage service discovery, brokering and authentication.

Service discovery agents constantly scan the cloud 'horizon' to detect the presence of new services that can be utilised by tenants. Within the set of available services, there is then a matching service that attempts to identify service availability and correlate this with service need. Finally, an agent that manages an authentication service can then start the process of establishing trust between parties, as illustrated in Figure 2.

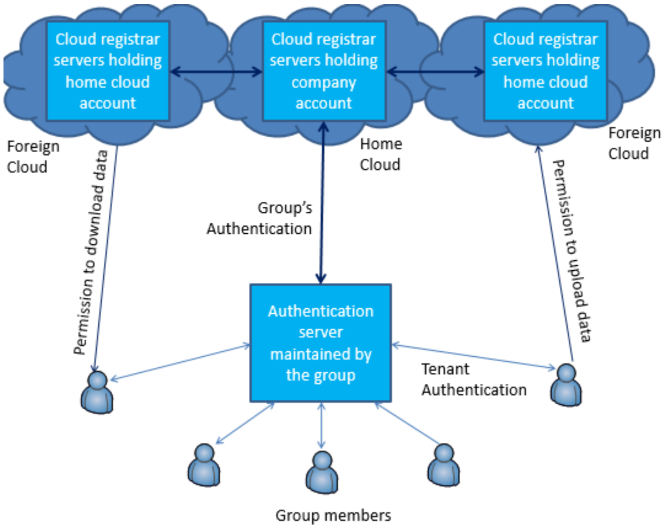
Cloud registrar servers holding home cloud account
Cloud registrar servers holding company account
Cloud registrar servers holding home cloud account
Foreign Cloud
Home Cloud
Foreign Cloud
Permission to download data
Group's Authentication
Permission to upload data
Authentication server maintained by the group
Tenant Authentication
Group members

Fig. 2. Hierarchical multi-party structure in multi-cloud computing [34].

Trust is established between the home and foreign clouds by the use of several keys, whose creation is invoked as a trigger for the relationship to be generated. Once this is in place, the home cloud can then marshall services, via the authentication cloud, to whichever collection of multiple parties that exists.

For a user to obtain trusted access to a resource, there now exists a process where they divulge private information for authentication, in order to create private keys as necessary. This identification, together with the group key, is then added to the key for the home cloud.

It is essential that secure information is exchanged in order to establish trust, but also to ensure that any redundancy and/or resilience is built into the scheme [52]. It might be that the home cloud could use attributes of tenants as a means of communicating an intention to create trust with foreign clouds, on the basis that the recipients themselves would manage and issue public keys, for later augmentation with personalised private keys as per the scheme described above.

In the IoT domain, the security controls that we are exploring will be impractical to manage manually. Automation is an essential enabler of a practical approach to trust between multiple parties [53], and the ability to rely on the operation of such services is of paramount importance to all parties.

The inherent complexity of combining services from multiple parties in an open world setting will inevitably lead to the identification of system errors, either before or after an effect is detected [53], [54]. These potential design flaws are compounded by the introduction of human behaviour and operation of the business systems, as such behaviours can be challenging to forecast accurately.

D. A multiparty authentication model

Prior work [34] describes a framework that addresses the challenges of providing the necessary agility for authorisation in a dynamic, multi-party setting. Figure 3 illustrates the framework in the context of a Session Authority Cloud that in this case is implemented as a Field Programmable Gate Array (FPGA), though it could also be a remote cloud. The role of the SAC is to marshall the individual sessions that are requested by any of the multiple parties (clouds).

The SAC does not distinguish between clouds, nor does it rely on them being classified as 'home' or 'foreign', and it maintains overall authority over any party that has a desire to join the system. Authentication data for all tenants is retained by the SAC, including root keys for example.

V. Physically Unclonable Functions

In recent years, PUF circuits have produced significant interest as promising hardware security primitives for low overhead security applications. A PUF is a hardware entity that is easy to use but hard to anticipate the behavior.

The design is practically not feasible to clone, even with the knowledge of the exact design and manufacturing process involved in its production. Due to this feature, PUFs have been a secure cryptographic substitute for traditional methods of random key generation and secure key storage.

In this work we use the XOR Arbiter PUF (XOR-APUF) which are popularly used for authentication and are efficiently implementable on FPGAs, making them an ideal choice for FPGA based security applications [55], [56]. APUF is formed by connecting an arbiter to a pair of parallel paths formed by the switches according to the state of challenge bits (see figure). This PUF consist of 'n' bit challenges and a single bit response. A standalone APUF is prone to modeling attacks based on machine learning [57].

As a security measure, we use an XOR- Arbiter PUF (see figure), with a composition of 10 or more APUFs instances XOR-ed to generate the response. This composition is proved to be resilient from machine learning attacks [58].

VI. Multi-party authentication using PUF

An FPGA (F) is configured with 'N' XOR-PUFs each constituting of 10 or greater number of Arbiter PUFs. The number 'N corresponds to the number of users in the network. Using secure dynamic partial reconfiguration (DPR), more PUFs can be configured in the FPGA, to permit any additional (dynamic) user.

We use Xilinx design tools and follow the approach discussed in [59] for developing partial bitstreams for reconfigurable PUFs. Reconfiguration is done dynamically over the network. Hardware updates over the network might bring potential threats in the form of malicious hardware alterations [60], [61].

We insist the usage of a secure partial reconfiguration over the network to prevent any malicious alterations of the device using hardware trojan insertion. Secure IoT hardware updates can also be done using an authentication protocol enabled by a PUF configured in the static partition of the device [6].

VII. Authentication Protocols

This algorithm provides a secure protocol to authorise a user in an IoT network without adopting explicit storage of keys at the IoT nodes (SAC-FPGA or a key vault). This is achieved using a PUF based protocol.

The method authorises an existing user (Protocol-1), as well as a new user using the properties of dynamic partial reconfiguration. A user is declared as genuine if he/she is introduced by an existing user. A dynamically reconfigurable XOR-arbiter PUF is the security module behind this algorithm.

The first part of the algorithm defines multiparty authorisation in a static environment. We define a static environment as a scenario in which all the requesting IoT nodes (users) are known to the network. The network contains 'N' users (existing) and 'K' IoT clouds.

The system contains a file handler, which processes and responds to requests between the user and a SAC FPGA. SAC-FPGA contains XOR-APUF configured in its fabric representing every authorised user in the network. The system consists of an evolvable framework, to begin with, we consider 'N' XOR-APUFs to be configured in the static part of the FPGA-fabric.

The static part corresponds to the FPGA fabric which is not expected to bring changes in future after deployment. The number of APUFs in the XOR-APUF is chosen to be strictly higher than 10 to avoid any modelling attacks based on machine learning techniques as described previously.

The FPGA-fabric also contains a dynamic partition, which could incorporate more PUFs (users) / or modify the existing PUF design for enhanced security. Addition of a new user using PUF-based authentication protocol will be discussed in the second phase of the algorithm.

Every authenticated user holds a mathematical model of the PUF. A mathematical model of the XOR-APUF with 10 or higher arbiter stages is configurable only with the knowledge of individual constituent arbiters. We assume that these modeling parameters are exchanged through a secure communication channel.

A. Protocol-1

User U_i in the static network requesting an authorisation for a session on the IoT cloud C_j should follow the following steps. The User U_i makes a request to the file handler asking an IoT session on Cloud C_j.

The find handler responds with a set of 'q' challenges, each of size 'r'. The file handler, for every user, maintains a database of challenges that have been previously used for PUF based DPR enabling/disabling, and disregards every old challenge used.

However, for challenge set size of 'q' in each authentication attempt, with each challenge being 'r'-bit, the probability of repeated challenges occurring termed as the "Failure Probability" is almost zero with a typical value of q=1000 and r=64 [6].

On applying the received challenges to the model M_i, the user produces the responses Rimp. The 'q' responses along with the user ID is concatenated to form a string, which is encoded with a previously agreed scheme (forms a certificate CA_i), and is send to the file handler.

The file handler sends the received certificate to the SAC-FPGA for verification. The SAC FPGA decodes the ID and the responses generated by the mathematical model of PUF P_i, residing with the user U_i. The SAC FPGA also receives the challenge bits from the file handler.

On applying the received challenges to the PUF P_i, the SAC FPGA produces the responses R_{ifp}.

The verification stage finds the match between the two responses.

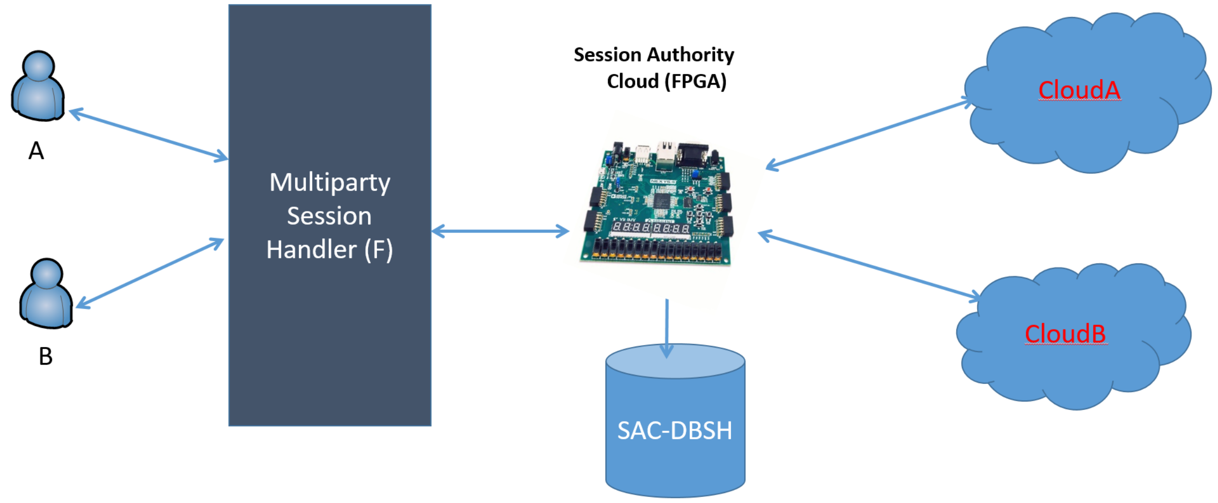
A
B
Multiparty Session Handler (F)
Session Authority Cloud (FPGA)
SAC-DBSH
CloudA
CloudB

Fig. 3. Proposed multiparty session authentication framework: The system consists of a session handler, who is responsible for handling the request of different users. The SAC-FPGA follows a secure authentication protocol to enable access to the various clouds. The FPGA used permits dynamic alteration of users in the network using dynamic partial reconfiguration. A PUF security primitive implemented on the FPGA is the key element of the secure multiparty authentication protocol.

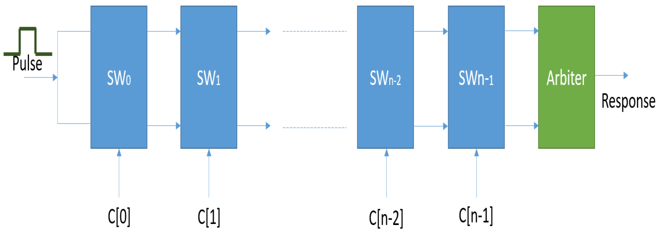

Fig. 4. Arbiter PUF: With n-bit challenge and a single bit response. An arbiter PUF compares two paths with an identical delay in design, where a random process variation determines which path is faster. Based on the fastest path, the arbiter outputs a 1-bit digital response.

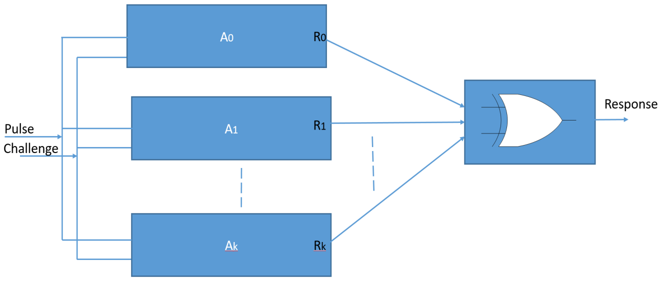

Fig. 5. XOR Arbiter PUF with k constituent PUFs: Arbiter PUFs are duplicated k-times to form an XOR Arbiter PUF. All the constituent arbiter PUFs are given the same challenge bits. The challenge bits select a unique delay path in determining the outcome of the arbiter. The multiple responses produced are then XOR-ed to generate a 1-bit digital response.

B. Protocol-2

The second part of the algorithm describes an evolving IoT network. This protocol is to enable a new user to access an IoT node after successful introduction by an existing user. A user UB,

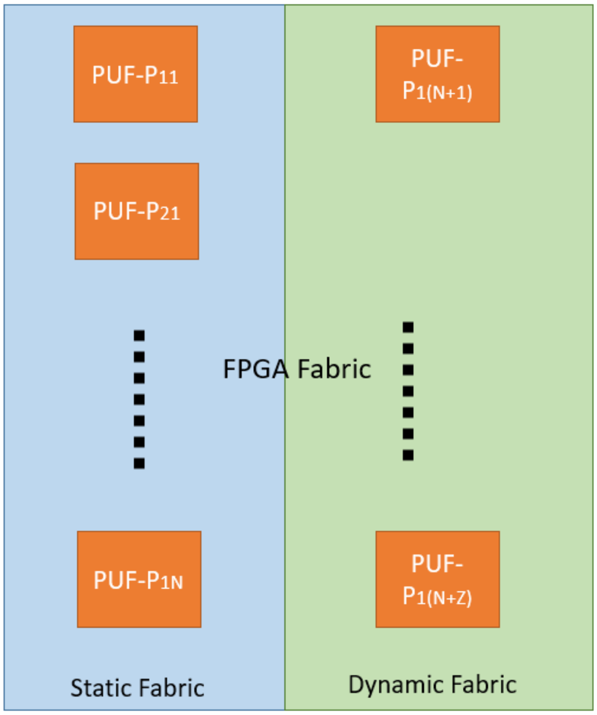

Fig. 6. FPGA fabric configured with PUFs: The FPGA fabric is divided into two regions- the static partition and the dynamic partition. The static partition consists of PUFs which are configured before deployment and with a fixed and unalterable design. New PUFs can be added to the dynamic partition as they evolve with time using dynamic partial reconfiguration feature of the FPGA. This evolution aids in incorporating dynamic users into the network by following a trusted multiparty authentication protocol.

requests an existing user, UA for an introduction to access a cloud, Ci. The user UB is known to UA as a trusted entity. The user UA requests that the file handler introduces the new user. The file handler responds with a set of challenge bits. The user UA applies the challenge bits to its model and forms a certificate CA, which is given to the user UB. User UB sends the certificate received from UA, with its ID number to the file handler. The file handler verifies if user A is genuine by comparing the responses of the PUF model and the physical PUF. If UA is successfully authenticated, the FPGA declares UB to be trustworthy.

Algorithm 1 User is a member of the cloud to be accessed

Objective:

(a) The session Authority Cloud is an FPGA which verifies the identity of user (U_{A}) who is requesting access.

(b) The FPGA provides session key for the genuine set of users (U_{i}).

Prerequisites

1) An n-bit input, 1-bit output XOR PUF P_1 is reconfigured in the static partition of the $SAC-FPGA$. There exists a PUF for every authenticated user. PUF P_1 represents the identity of the user.
2) Each user also has an identity number, ID.
3) A mathematical model M_{i} of P_{i} resides with each User.
4) F and user U_{i} have agreed on a fixed encoding scheme $E(.)$ and a decoding scheme $D(.)$, such that for any binary string $x, E(.)$ and $D(.)$ are injective, $X = E(x)$ and $D(X) = x$.

Output A value in variable $Flag$ to show that the session is granted ($Flag = 1$) or denied ($Flag = 0$).

Steps

```
1: $U_{\mathrm{i}}$ to File handler $F$ : request Access to IoT cloud $Cj$
2: $F$ to $U_{\mathrm{i}}$ : Request for the identity number ID of the user and responds to a set of challenges $CH_{\mathrm{p}}$. $F$ sends $q$ challenge bits each of length $n$ to $U_{\mathrm{i}}$.
3: $Ui$ calculates the following: $Rim_{\mathrm{p}} = Mi(CH_{\mathrm{p}})$, $p = 1q$, $Rim = (Rim_1, Rim_2, Rim_3, Rim_{\mathrm{q}})$, $CA_{\mathrm{i}}$=$E(ID_{\mathrm{i}}, Rim)$
4: $U_{\mathrm{i}}$ to $F$ : $U_{\mathrm{i}}$ sends the certificate $CA_{\mathrm{i}}$ to $F$
5: $F$ generates a session ID for the IoT cloud access.
6: $F$ to $SAC-FPGA$: $F$ sends the set of challenges $CH_{\mathrm{p}}$ and $CA_{\mathrm{i}}$ to the $SAC-FPGA$
7: $SAC-FPGA$ calculates the following
   a $(ID, Rim) = D(CA_i)$
   b $R_{ifp} = P_i(CH_p), p = 1q$
   c $N_i = (1 - \frac{\sum_{(p=1)}^{q}(R_{imp} \bigoplus R_{ifp}}{q})$ If $Ni \geq 0.99$, $SAC-FPGA$ declares $U_{\mathrm{i}}$ as an authenticated user.
8: $SAC$ to $IoT$ cloud. Flag indicating $U_{\mathrm{i}}$ is authenticated or not. Sends the $SessionID$ and $UserID$ to to the $IoT$ Cloud $C_{\mathrm{j}}$ if authenticated.
9: Cloud $C_{\mathrm{j}}$ approves the decision to grand session for authenticated user $U_{\mathrm{i}}$. $Flag = 1$ and exit.
```

Algorithm 2 User is not a member of the cloud to be accessed

Objective:

(a) The Session Authority Cloud is an FPGA which verifies the identity of user (U_{B}) who is requesting access.

(b) The FPGA provides session key for the genuine set of new users ($\mathrm{U_i}$).

Prerequisites

1) SAC FPGA has built-in controllers to facilitate secure dynamic partial reconfiguration.
2) FPGA fabric is divided into two parts, a) static fabric and b) dynamic fabric. Static fabric consists of PUF configurations which existed before deployment. They might be assigned to some set of genuine users in the beginning. The dynamic fabric is dedicated to configure additional security primitives (mostly PUFs) for any genuine dynamic user using secure dynamic partial reconfiguration.

Output A value in variable $Flag$ to show that a session is granted ($Flag = 1$) or denied ($Flag = 0$).

Steps

```
1: $U_{\mathrm{B}}$ requesting introduction to $U_{\mathrm{A}}$ to access the cloud $C_{\mathrm{j}}$
2: $U_{\mathrm{A}}$ to File handler $F$: request introduction of $U_{\mathrm{B}}$ to cloud $C_{\mathrm{j}}$
3: F to $U_A$: Request for keys for authentication by sending a set of challenges $CH_p$. There are ‘q’ challenge bits each of length ‘n’.
4: $UA$ calculates the following:
   a $RAmp = MA(CHp), p = 1q$
   b $RAm = (RAm1, RAm2, RAm3, RAmq)$
   c $CAA = E(IDA, RAm)$
5: $UA$ to $UB$ $UA$ sends the certificate $CAA$ to $UB$
6: $UB$ to F: E(IDB,IDA,CAA)
7: F to SAC-FPGA: F new user request IR, set of challenges CHp and CAA to the SAC-FPGA
8: SAC-FPGA calculates the following
   a $RAm = D.(CAA)$
   b $RAfp = PA(CHp), p = 1q$
   c $N_A = (1 - \frac{\sum_{(p=1)}^{q}(R_{Amp} \bigoplus R_{Afp}}{q})$, If $N_A \geq 0.99$, SAC-FPGA declares $U_A$ as an authenticated introducer and $U_B$ as a genuine user.
9: SAC FPGA configures new PUFs $P_B$ using secure dynamic partial reconfiguration in the dynamic part of the FPGA.
10: SAC-FPGA to $U_B$: sends PUF modelling parameters ‘m’ through secure channel
11: $U_B$ constructs the mathematical model $M_B$ of the PUF $P_B$ from ‘m’
12: Now $U_B$ is same as any other user. $Flag = 1$ and exit and follow protocol-1.
```

This initiates a dynamic partial reconfiguration (DPR) process, which adds configures a new PUF in the dynamic part of the FPGA fabric. We assume that a secure DPR process is followed.

The FPGA sends the modeling parameters to UB, through a secure channel, enabling the mathematical modelling of the PUF. Now user UB is same as any other existing user, and has to follow protocol 1 to gain access to the IoT cloud.

VIII. Conclusions and Future Work

Security has always been a concern for companies targeting the IoT and its many applications, as well as the developers who need the resources to help ensure they can deliver products that will meet their customers' requirements. With the use of cryptography in embedded devices increasing, semiconductor manufacturers are seeing improved demand with innovative solutions aimed at ensuring that IoT meets and probably exceeds their expectations.

This article has considered problems associated with reliable, timely and secure data transfer mechanisms necessary for shared business data processing networks.

This multiparty authentication system for dynamic authentication interactions is effective when members of different security realms want to access distributed business data micro services [62] through a trusted principal.

Our proposed mechanism can help cloud session users authenticate their session membership so as to largely simplify the authentication processes within multi-party sessions.

While this paper has presented the framework, additional research and development will develop a set of protocols for multi-party session management and cross-realm authentication for dynamic authentication interactions, between users and data services in multiple cloud systems located in different security realms.

The scenario of multiparty authentication across security realms is not limited to business processes that require access to data services. Internet of Things (IoT) architectures are a contemporary example of a need to be able to model, comprehend and deploy authentication mechanisms that can securely tolerate myriad network nodes that each provide more cohesive services [2].

We are now progressing the work in two ways.

First, we are formally evaluating the authentication protocols in order to robustly deploy the framework to an environment that is composed of a mixed set of discrete devices, enabling the framework to be tolerant of existing and emerging technologies for cloud platforms and network infrastructures.

Second, we are now including a variety of devices in addition to clouds within the simulation, to better understand the effects upon network performance when greater numbers of low powered computing and storage wireless nodes are introduced [63].

This replicates the emerging IoT and Industrial IoT scenarios where extensive integration of Wireless Sensor Networks and edge computing nodes is commonplace.

Acknowledgment

This work has been supported by the Centre for Industrial Analytics (CIndA) at the University of Huddersfield, UK.

References

[1] A. J. Jara, M. A. Zamora-Izquierdo, and A. F. Skarmeta, "Interconnection Framework for mHealth and Remote Monitoring Based on the Internet of Things," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 47–65, 2013.

[2] A. Ikram, A. A., and N. L. L. S. S. Hill, R.and Antonopoulos, "Approaching things (IoT): a Modelling, Analysis and Abstraction Framework," *Concurrency and Computation: Practice and Experience*, pp. 1966–1984, 2015.

[3] M. Chui, M. Löffler, and R. Roberts, "The Internet of Things," 2010.

[4] K. Hwang and M. Chen, *Big-data Analytics for Cloud, IoT and Cognitive Computing*. John Wiley & Sons, 2017.

[5] W. Lie and W. Feng-Yan, "Dynamic Partial Reconfiguration in FPGAs," in *2009 Third International Symposium on Intelligent Information Technology Application*, vol. 2. IEEE, 2009, pp. 445–448.

[6] A. P. Johnson, R. S. Chakraborty, and D. Mukhopadhyay, "A PUF-enabled Secure Architecture for FPGA-based IoT Applications," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 110–122, 2015.

[7] *Vivado Design Suite Tutorial–Partial Reconfiguration UG947 (v2018.3)*, Xilinx Inc, [Online]. Available: www.xilinx.com/support/documentation/sw_manuals/xilinx2018_3/ug947-vivado-partial-reconfiguration-tutorial.pdf, 2019, accessed: 2019-05-21.

[8] A. Sajid, H. Abbas, and K. Saleem, "cloud-assisted iot-based scada systems security: A review of the state of the art and future challenges," *IEEE Access*.

[9] E. Trichina, M. Bucci, D. De Seta, and R. Luzzi, "Supplemental Cryptographic Hardware for Smart Cards," *IEEE micro*, vol. 21, no. 6, pp. 26–35, 2001.

[10] M. Canim, M. Kantarcioglu, and B. Malin, "Secure Management of Biomedical Data with Cryptographic Hardware," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 1, pp. 166–175, 2011.

[11] T. W. Arnold, C. Buscaglia, F. Chan, V. Condorelli, J. Dayka, W. Santiago-Fernandez, N. Hadzic, M. D. Hocker, M. Jordan, T. Morris *et al.*, "IBM 4765 Cryptographic Coprocessor," *IBM Journal of Research and Development*, vol. 56, no. 1.2, pp. 10–1, 2012.

[12] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in *2007 44th ACM/IEEE Design Automation Conference*. IEEE, 2007, pp. 9–14.

[13] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[14] D. Mukhopadhyay, "PUFs as Promising Tools for Security in Internet of Things," *IEEE Design & Test*, vol. 33, no. 3, pp. 103–115, 2016.

[15] H. Al-Aqrabi, L. Liu, R. Hill, L. Cui, and J. Li, "Faceted Search in Business Intelligence on the Cloud," in *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*. IEEE, 2013, pp. 842–849.

[16] P. Sundararajan, "High Performance Computing using FPGAs," *Xilinx white paper: FPGAs*, pp. 1–15, 2010.

[17] C. De Schryver, *FPGA Based Accelerators for Financial Applications*. Springer, 2015.

[18] M. A. H. Dempster, J. Kanniainen, J. Keane, and E. Vynckier, *High-Performance Computing in Finance: Problems, Methods, and Solutions*. CRC Press, 2018.

[19] T. Wollinger and C. Paar, "How Secure are FPGAs in Cryptographic Applications?" in *International Conference on Field Programmable Logic and Applications*. Springer, 2003, pp. 91–100.

[20] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, "Hardware Trojan: Threats and Emerging Solutions," in *2009 IEEE International high level design validation and test workshop*. IEEE, 2009, pp. 166–171.

[21] A. P. Johnson, S. Saha, R. S. Chakraborty, D. Mukhopadhyay, and S. Gören, "Fault Attack on AES via Hardware Trojan Insertion by Dynamic Partial Reconfiguration of FPGA over Ethernet," in *Proceedings of the 9th Workshop on Embedded Systems Security*. ACM, 2014, p. 1.

[22] H. Liu, H. Ning, Q. Xiong, and L. T. Yang, "Shared Authority based Privacy-preserving Authentication Protocol in Cloud Computing," *IEEE Transactions on parallel and distributed systems*, vol. 26, no. 1, pp. 241–251, 2014.

[23] H. Al Aqrabi, L. Liu, R. Hill, and N. Antonopoulos, "A Multi-layer Hierarchical Inter-Cloud Connectivity Model for Sequential Packet Inspection of Tenant Sessions Accessing BI as a Service," in *2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC, CSS, ICESS)*. IEEE, 2014, pp. 498–505.

[24] K.-K. R. Choo, O. F. Rana, and M. Rajarajan, "Cloud Security Engineering: Theory, Practice and Future Research," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 372–374, 2017.

[25] G. Ateniese, M. Steiner, and G. Tsudik, "New Multiparty Authentication Services and Key Agreement Protocols," *IEEE journal on selected areas in communications*, vol. 18, no. 4, pp. 628–639, 2000.

[26] J. Katz and M. Yung, “Scalable Protocols for Authenticated Group Key Exchange,” in *Advances in Cryptology - CRYPTO 2003*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 110–125.

[27] Y. Rahulamathavan, R. C.-W. Phan, S. Veluru, K. Cumanan, and M. Rajarajan, “Privacy-preserving Multi-class Support Vector Machine for Outsourcing the Data Classification in Cloud,” *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 5, pp. 467–479, 2013.

[28] E.-J. Yoon and K.-Y. Yoo, “New Authentication Scheme based on a One-way Hash Function and Diffie-Hellman Key Exchange,” in *International Conference on Cryptology and Network Security*. Springer, 2005, pp. 147–160.

[29] D. Thilakanathan, S. Chen, S. Nepal, and R. A. Calvo, “Secure Data Sharing in the Cloud,” in *Security, Privacy and Trust in Cloud Systems*. Springer, 2014, pp. 45–72.

[30] W. Song, H. Zou, H. Liu, and J. Chen, “A Practical Group Key Management Algorithm for Cloud Data Sharing with Dynamic Group,” *China Communications*, vol. 13, no. 6, pp. 205–216, 2016.

[31] P. K. Arya, K. Selvamani, S. Kanimozhi, and A. Kannan, “Data Sharing for Dynamic Group in the Cloud Environment by using Group Signature Approach,” 2013.

[32] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, “Security and Cloud Computing: Intercloud Identity Management Infrastructure,” in *2010 19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises*. IEEE, 2010, pp. 263–265.

[33] D. Georgakopoulos, M. Hornick, and A. Sheth, “An Overview of Workflow Management: From Process Modeling to Workflow Automation Infrastructure,” *Distributed and parallel Databases*, vol. 3, no. 2, pp. 119–153, 1995.

[34] H. Al-Aqrabi and R. Hill, “Dynamic Multiparty Authentication of Data Analytics Services Within Cloud Environments,” in *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, June 2018, pp. 742–749.

[35] J. D. Clercq, “Single Sign-On Architectures,” in *Proceedings of the International Conference on Infrastructure Security*, ser. InfraSec ’02. London, UK, UK: Springer-Verlag, 2002, pp. 40–58.

[36] C. Baker, A. Anjum, R. Hill, N. Bessis, and S. L. Kiani, “Improving Cloud Datacentre Scalability, Agility and Performance Using OpenFlow,” in *2012 Fourth International Conference on Intelligent Networking and Collaborative Systems*, Sep. 2012, pp. 20–27.

[37] M. U. Yaseen, A. Anjum, O. Rana, and R. Hill, “Cloud-based Scalable Object Detection and Classification in Video Streams,” *Future Gener. Comput. Syst.*, vol. 80, no. C, pp. 286–298, Mar. 2018.

[38] S. Hada and H. Maruyama, “Session Authentication Protocol for Web Services,” in *Proceedings 2002 Symposium on Applications and the Internet (SAINT) Workshops*, Jan 2002, pp. 158–165.

[39] R. Roman, P. Najera, and J. Lopez, “Securing Things,” *Computer*, vol. 44, no. 9, pp. 51–58, Sep. 2011.

[40] H. Al-Aqrabi, L. Liu, R. Hill, Z. Ding, and N. Antonopoulos, “Business intelligence security on the clouds: Challenges, solutions and future directions,” in *2013 IEEE Seventh International Symposium on Service-Oriented System Engineering*, March 2013, pp. 137–144.

[41] A. Kanuparthi, R. Karri, and S. Addepalli, “Hardware and embedded security in the context of internet of things,” in *Proceedings of the 2013 ACM Workshop on Security, Privacy &#38; Dependability for Cyber Vehicles*, ser. CyCAR ’13. ACM, 2013, pp. 61–64.

[42] “Gartner Says 8.4 Billion Connected ”Things” Will Be in Use in 2017, Up 31 Percent From 2016,” [Online]. Available:https: //www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016, Feb 2017, accessed: 2019-05-23.

[43] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, “Security and Cloud Computing: InterCloud Identity Management Infrastructure,” in *2010 19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises*, June 2010, pp. 263–265.

[44] R. Sharma and B. Joshi, “H-IBE: Hybrid-identity based Encryption Approach for Cloud Security with Outsourced Revocation,” in *Inter-*

[45] C. Schridde, T. Drnemann, E. Juhnke, B. Freisleben, and M. Smith, “An identity-based security infrastructure for cloud environments,” in *2010 IEEE International Conference on Wireless Communications, Networking and Information Security*.

national Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Oct 2016, pp. 1192–1196.

[46] J. Li, B. Li, T. Wo, C. Hu, J. Huai, L. Liu, and K. Lam, “CyberGuarder: A Virtualization Security Assurance Architecture for Green Cloud Computing,” *Future Generation Computer Systems*, vol. 28, no. 2, pp. 379 – 390, 2012.

[47] H. Al-Aqrabi, L. Liu, R. Hill, and N. Antonopoulos, “Cloud bi: Future of business intelligence in the cloud,” *Journal of Computer and System Sciences*, vol. 81, no. 1, pp. 85 – 96, 2015.

[48] M. Burrows, M. Abadi, and R. Needham, “A Logic of Authentication,” *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, Feb. 1990.

[49] C.-Y. Chen and J.-F. Tu, “A Novel Cloud Computing Algorithm of Security and Privacy,” *Mathematical Problems in Engineering*, pp. 1–6, 2013.

[50] S. Pippal, V. Sharma, S. Mishra, and D. S. Kushwaha, “An Efficient Schema Shared Approach for Cloud Based Multitenant Database with Authentication and Authorization Framework,” in *2011 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, Oct 2011, pp. 213–218.

[51] H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-Based Authentication for Cloud Computing,” in *IEEE International Conference on Cloud Computing*. Springer, Berlin, Heidelberg, 2009, pp. 157–166.

[52] H. Li, Y. Dai, and B. Yang, *Identity-Based Cryptography for Cloud Security*, University of Electronic Science and Technology of China and University of Tennessee, USA, [Online]. Available: https://eprint.iacr.org/2011/169.pdf, 2019, accessed: 2019-05-21.

[53] B. Qin, H. Wang, Q. Wu, J. Liu, and J. Domingo-Ferrer, “Simultaneous Authentication and Secrecy in Identity-based Data Upload to Cloud,” *Cluster Computing*, vol. 16, no. 4, pp. 845–859, Dec. 2013.

[54] S. Sotiriadis, N. Bessis, N. Antonopoulos, and R. Hill, “Meta-scheduling Algorithms for Managing Inter-cloud Interoperability,” *Int. J. High Perform. Comput. Netw.*, vol. 7, no. 3, pp. 156–172, Sep. 2013.

[55] M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach, and S. Devadas, “Slender PUF Protocol: A Lightweight, Robust, and Secure Authentication by Substring Matching,” in *2012 IEEE Symposium on Security and Privacy Workshops*, May 2012, pp. 33–44.

[56] M. Barbareschi, P. Bagnasco, and A. Mazzeo, “Authenticating IoT Devices with Physically Unclonable Functions Models,” in *2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, Nov 2015, pp. 563–567.

[57] U. Rhrmair, J. Slter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, “PUF Modeling Attacks on Simulated and Silicon Data,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1876–1891, Nov 2013.

[58] J. Tobisch and G. T. Becker, “On the scaling of machine learning attacks on pufs with application to noise bifurcation,” in *Revised Selected Papers of the 11th International Workshop on Radio Frequency Identification - Volume 9440*, ser. RFIDsec 2015. Springer-Verlag New York, Inc., 2015, pp. 17–31.

[59] S. Gren, O. Ozkurt, Y. Turk, A. Yildiz, and H. F. Ugurdag, “enabling difference-based dynamic partial self reconfiguration for large differences,” in *2013 8th IEEE Design and Test Symposium*.

[60] A. P. Johnson, R. S. Chakraborty, and D. Mukhopadhyay, “A PUF-Enabled Secure Architecture for FPGA-Based IoT Applications,” *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 110–122, April 2015.

[61] A. P. Johnson, S. Patranabis, R. S. Chakraborty, and D. Mukhopadhyay, “Remote Dynamic Partial Reconfiguration: A Threat to Internet-of-Things and Embedded Security Applications,” *Microprocessors and Microsystems*, vol. 52, pp. 131 – 144, 2017.

[62] D. Shadija, M. Rezai, and R. Hill, “Towards an Understanding of Microservices,” in *2017 23rd International Conference on Automation and Computing (ICAC)*, Sep. 2017, pp. 1–6.

[63] J. M. Garca-Campos, D. G. Reina, S. L. Toral, N. Bessis, F. Barrero, E. Asimakopoulou, and R. Hill, “Performance Evaluation of Reactive Routing Protocols for VANETs in Urban Scenarios Following Good Simulation Practices,” in *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, July 2015, pp. 1–8.