ASTES

*Advances in Science, Technology and Engineering Systems Journal Vol. 3, No. 5, 46-55 (2018)*

*www.astesj.com*

*Special Issue on Multidisciplinary Sciences and Engineering*

**ASTESJ**

**ISSN: 2415-6698**

# Holistic Access Control and Privacy Infrastructure in Distributed Environment

Uche Magnus Mbanaso[1,*], Gloria A Chukwudebe[2]

[1]*Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria*

[2]*Department of Electrical & Electronic Eng., Federal University of Technology Owerri, Nigeria*

ARTICLE INFO

*Article history:*
*Received: 18 August, 2018*
*Accepted: 27 October, 2018*
*Online: 01 November, 2018*

*Keywords:*
*Internet*
*Internet of Things*
*Cyber- physical system*
*Digital trust,*
*Confidentiality,*
*Privacy*
*Access Control*
*Distributed Environment*

ABSTRACT

*This article discusses IoT security in situations whereby devices do not share the same security domains, which raises security, privacy and safety concerns. It then presents an Access Control and Privacy infrastructure for addressing these concerns in the context of distributed environments. IoT deployments allow billions of connected physical devices to collect, process and share data; collaborate and cooperate in automating tasks in an unrivaled fashion. However, security and safety are still top major fears that demand holistic approach, particularly when devices do not share the same digital trust. This is not a surprise, as a revolutionary system, IoT comes with inherent vulnerabilities, threats and risks like most other computing and data processing systems. Conversely, when security breaches or compromises occur, it is most likely to have a far-reaching and upsetting consequences that extends traditional concerns. The fact that IoT can be deployed in plethora of application scenarios; means that end-to-end security should be treated contextually and in a dynamic manner. Consequently, these concerns; trust, confidentiality, and privacy at the IoT application stack need to be addressed robustly. Thus, in this article, a novel distributed access control infrastructure based on configurable policy constructs is presented. The infrastructure provides a mechanism for gradual negotiated release of provable attributes to dynamically build trust before protected resources are made available. In this configuration, IoT transaction parties can express their Capabilities (competences, features, etc.) and Requirements (rules and provable attributes required to access the capabilities) as the basis for sharing data or collaboration in solving business problems.*

## 1. Introduction

This paper is an extension of work originally presented during the 13th International Conference on Electronics, Computer and Computation (ICECCO) in 2017 [1]. The deployment of Internet of Things (IoT) is developing in many areas and contexts. Its deployment spans across diverse spaces and is anticipated to continue to extend beyond present expectations [2]. In some deployments, the range of IoT devices that may work together or share data are unlikely to belong to a single (or the same autonomous) security domain [3]. By security domain, we basically mean a collection of connected entities or applications that are part of a specific digital trust infrastructure (or administered by common cryptographic policy), i.e. Public Key Infrastructure (PKI) security arrangement for authentication, authorization and session management. Invariably, when devices, which are members of different security domains want to collaborate in providing business solutions, it raises trust, confidentiality and privacy challenges in a variety of application contexts. This demands fresh security requirements as threats posed by cyber, physical and human factors span beyond traditional risk landscapes. However, trust, confidentiality and privacy have received substantial attention in the literature in different contexts [4][5][6][3][7].

Notwithstanding, IoT has different set of physical and virtual (or logical) fresh crop of security issues that varies, and are contextually multifaceted. That is, IoT security, privacy and safety may be seen from a variety of surfaces including those specific to the device, cloud computing, mobile apps, network interfaces, software, physical and access control. While a number of these security areas, can be addressed specifically by vendors and/or manufacturers, yet some have to be addressed in application context and real-time, and cannot be on the basis of 'one solution fits all'. Arguably, it requires security infrastructure

*Uche Mbanaso, Centre for Cyberspace Studies, Nasarawa State University, Keffi, Email: ozara.oru@gmail.com

that is adaptable and flexible, taking into consideration the business or solution environments. It therefore aptly suggests that IoT operational environments can be highly contestable with several attack opportunities for intruders. This raises strong digital trustworthiness as germane for treating identity and access management in emerging smart environments. The assurance of how data is collected, processed and shared, entails an obligation to mutually respect contractual data access agreements that met security principles and privacy.

A typical example can buttress our point. A smart vehicle arriving a city would like to request certain city-based data from available connected city IoT systems [2]. But a secure conversation will demand that these city devices cannot wittingly disclose data without first ascertaining the trustworthiness of such third party entity. It is assumed here that the smart vehicle belongs to another security domain and has no existing digital trust affiliation with the city's security domain[8]. For security and safety purpose, both parties should exchange information based on the ability to trust each other[9][10]. It implies that access and data security as well as safety of these connected entities must be reciprocally assured. Inversely, the smart vehicle may equally not be ready to disclose its profile to the city systems straight away, and the city systems cannot assume that the smart vehicle's mission is harmless, and thus share data with the vehicle or conduct operations together. In either direction, both parties have security, privacy and safety issues of concerns. In this regard, critical challenges can be inferred as follows:

- Unauthorised activities of hostile entities to compromise security and safety of IoT;
- Activities of friendly parties to disregard mutually contractual agreements to violate security and safety of devices, resources or underpinning infrastructure.

To this extent, IoT security and safety landscapes are still evolving issues constrained by encumbrances that have both socio-economic and security impetus. Furthermore, privacy and trust are subjective to cultural perceptions with unpredictable degree of individual capacity and expectations [11]. Unlike trust that is by no way regulated, privacy rights are subjective to some sort of regulations, especially by legislation, security principles, procedures, ethics, etc. in a variety of countries [12][13]. Aside, it is expected that a blanket access cannot be allowed to typical IoT systems, particularly for safety reasons; besides the need to secure sensitive resources and/or attributes. This, uniquely makes a further strong case for a symmetric security infrastructure at application stack that supports fine-grained policy in decision-making and authorization.

Therefore, it is obvious that IoTs are likely to operate in a variety of security domains and without pre-established digital trust but may have to share data, and where possible work together to address common business issues but in a secure and trusted manner. Thus, it is incumbent that identity and access management at application stack are critical requirement for treating security, privacy and safety. In this light, we present a bilateral symmetric and configurable policy-based infrastructure to address this critical application layer security in IoT distributed systems. This infrastructure uses Obligation of Trust (OoT) protocols[3] that allows reciprocated interexchange of policy constructs described as *Requirements* and *Capabilities* to gradually establish dynamic trust before making available protected information or performing some mutual tasks. Traditional solutions assume a form of digital trust based on simple use of username/password pair, which is highly susceptible to a variety of threats [14][15][16]. This is not ideal in many of IoT solution space, particularly in distributed environments.

Our solution is novel in many respects. First, it offers a real-time mutual treatment of security and privacy using configurable policy constructs that permits both parties in transaction to reciprocally take access decision based on their individual security requirements and capabilities. Second, it is a departure from one-way protection perception whereby only the security concerns of the party providing services is considered. Third, it is a highly scalable access control mechanism that has the capability to deal with present and future threats through robust and extensible rule constraints. Fourth, by addressing trustworthiness in privacy protection in a unified fashion, the infrastructure provides mechanisms for accountability, trust-based digital evidence as basis for dispute resolution, which is a critical requirement for IoT security and safety.

The rest of the paper is organized as follows: Section II reviews related works while Section III presents threat analysis and challenges in the context of privacy, trust and confidentiality. Section IV describes the novel Distributed Access Control Infrastructure while Section V presents discussions on the novel infrastructure. Section VI concludes the paper.

## 2. Review of Related Works

IoT requires a holistic approach to solve security, privacy and safety concerns in a particular security layer. This may entail combining technical, procedural and legal controls to minimize the severity of risks associated with access and availability of protected data as well as intellectual or proprietary property [1][3]. IoT operations take place at application stack where systems collect, store, analyze and share data. In some cases, sensitive attributes of service requesting parties are required to perform authorization. Undisputedly, privacy is most often considered from simple legal statements without automation of enforceable technical measures. Meanwhile IoT application level security is similar to those faced by other computing application space, existing identity and access control models can be adapted to suit IoT environments. However, the complexity is that an autonomous security domain may have hundreds or even thousands of connected objects with sensors and actuators to manage. This is the differentiator, which makes IoT risk landscape differ significantly. To this extent, the challenge before us is how to extend and adapt existing models and controls to address numerous IoT security issues. In the section that follows, security models and standards that influenced our solution are reviewed.

### *2.1. IoT Reference Model*

The increasingly broad adoption of IoT devices span wide area of use cases across multiple business domains including smart cities, smart manufacturing, smart agro, smart parks, smart hospitals, smart patient supported living solutions, etc.[17].

In smart cities, for instance, IoT sensors can focus on sensing the environment on some crowded areas. For instance, sensors can be used to ascertain air quality among others in an effort to monitor particular densely inhabited city zones periodically [18]. However,

sensor data can be spoofed or can become attack vector to facilitate a particular threat. In this context, understanding the tenets of security, privacy and safety issues is incumbent to the different IoT security layers. Thus, the IoT reference models create a common understanding of operational layers, features and functionality of IoT, which can help in insightful conceptualisation security architecture [18]. More importantly, it is instructive to note that no single security layer is a complete solution. However, there are plethora of IoT reference architectures, which helped to conceptualise IoT security[18][14][19].

*2.2. Federated Identity Management (FIM)*

Simply, the Federated Identity Management (FIM) is an infrastructure model used to associate identity information and attributes of entities across trusted several security domains [20]. The approach provides a mechanism for "single sign-on" in a fashion that allows transaction parties to obtain trusted access tokens from their local Identity Provider in order to be allowed access to outside services in a confederated manner [10][21]. An example of the FIM is the OpenID [22]. Usually, FIM is a classical transient trust built by using username/password pair to authenticate to a party's local Identity Provider (IdP) while this IdP issues and communicates signed access control assertions or tokens to the service providing party.

In some deployments, Attribute Authority (AA) is an integral part of FIM developed to provide a much more resilient access control engine as opposed to simple authentication provisions [23][24]. Typically, AA is simply, a trusted repository for secure storage of attributes/properties of parties commonly used in Attribute-Based Access Control (ABAC) infrastructure [20]. In some use cases, FIM attempts to distinguish authentication operations from authorization process on the basis of separation of security duties.

Although FIM offers user convenience and efficiency in managing identity provisions, users and relying parties, the use of username/password pair makes it defenseless against numerous threats. More so, issuance of access tokens is not on itself sufficient to guarantee the behaviour of a transaction entity. However, managing vast IoT identities has been raised as also a contending issue due to the anticipated volume of IoTs. Thus, FIM is potentially well suited for managing IoT identities, and as an integral part of a distributed access control infrastructure.

*2.3. eXtensible Access Control Markup Language (XACML)*

The XACML is a standard access control policy construct developed by the Organization for the Advancement of Structured Information Standards (OASIS), that provides collective framework for specifying a range of access control rules [25]. It has its foundation from eXtensible Markup Language (XML), and presents an extensive access control structure and encoding schemes to describe fine-grained access control rules as well as message level request-response construct that allow constituent part to work together in distributed access control operations. It exemplifies a modular infrastructure that is loosely coupled based on functionality and application domain, in a manner that allows them to be hosted independently.

*2.4. Security Assertion Markup Language (SAML)*

SAML is a very powerful and extensible language based on XML scheme specifically developed for the exchange of access control information from one transaction party to another. Usually, an identity provider (a SAML issuer or SAML authority) makes one or more assertion statements about a principal or entity in an opaque string, which is communicated to a consuming party, typically a service provider to grant access to the subject described on the digitally signed assertion [26][27]. The relying party decides to trust the SAML issuer based on some pre-existing trust relationship provided by digital certificate, which asserts that the subject is trustworthy.

From purely technical perspective, SAML assertion is the primary standard used by most single sign-on (SSO) schemes, even the FIM. The XML structure has an Issuer element that describes the SAML authority; the *Signature* section that holds the *signature block,* which encapsulate the PKI information of the issuer, algorithms and transforms as well as the resulting digital signature, etc. The *Subject* element encapsulates the identity of the subject; the *Condition* element describes obligatory conditions as an additional rule constraints. The *Assertion Statement* specifies the assertion context including authentication, attribute, authorization decision, or other user-defined constructs that can facilitate access control.

*2.5. Obligation of Trust (OoT) Protocol*

The Obligation of Trust Protocol (OoT) provides an innovative symmetric access control protocol as described in [7][28], which illustrates a bilateral and symmetric method that combines digital trust negotiation and access control operations for the treatment of security and privacy protections based on enforcement of mutual policy rules between two or more parties in distributed application environments. Ideally, the OoT protocol allows two or more transaction parties to interexchange policy constructs contained in *Requirements* and *Capabilities* in real-time. The OoT SAML request message described as a *Notification of Obligation* (NoB), first notifies the services requesting party the conditions for accessing its resources expressed as *Requirements* and its available services or features in *Capabilities.* The response message after execution of *Matching Algorithms* is the assurances that describes the fulfillment of each other's conditions contained in the *Requirements* policy element. The response message is characteristically the *Signed Acceptance of Obligations* (SAO). The details of OoT access control protocol that demonstrates how parties in conversation can use SAML Obligation of Trust Assertion can be found in [3][7].

## 3. Threat Analysis and Challenges

Fundamentally, to understand operational IoT security and safety issues, all layers of IoT must be considered and thoroughly assessed. Thus, the five security goals i.e. confidentiality, integrity, availability, authenticity, and non-repudiation should form the basis to assess threats. Consequently, in assessing these threats, three classic IoT system threats are described as follows:

- **A Target of an Attack**

Conventionally, an IoT device is potentially exposed to many threats faced by a typical computing system, particularly at network and application layers. It implies that IoT can suffer data breach or the device can be degraded, which can result to violation of confidentiality (or privacy) and integrity, as well as denial of service (availability). Most IoT systems have in-built application servers that equally face the same security challenges as traditional web servers[29]. OWASP[30], described ten top categories of IoT vulnerabilities that can be exploited by a hostile

party. Thus, threats can materialize through evading authentication provisions due to weak configurations and associations to the extent that it is too difficult to repudiate (non-repudiation) the nefarious actions. The extent to which this can happen depends on the mission, capability and the motivation of a hostile party.

- **A Tool for an Attack**

The composition of an IoT device includes sensors and actuators, implying the potential to be manipulated intelligently to distribute nefarious programmes or become an integral part of a malicious network that can take part in Distributed Denial of Service (DDoS) attack to cause unavailability. Likewise, operationally, an IoT can simplify a variety of attacks as sensors and actuators can conveniently become attack vectors. A malicious party can leverage unpretentious IoT operations for illegitimate purposes. In this context, such attacks may include undercover use of IoT engine to perpetuate cybercrime, financial fraud or cyberwarfare.

- **Incidental to an Attack**

This type of threat becomes possible when an IoT ecosystem is indirectly involved in an attack (i.e. stealthily supports criminal activities such as when in itself it is used to store data for criminal activities). It infers that possibly, an IoT can expedite an attack to occur much quicker by leveraging its power or functionality, or operational processes, which can make an attack more challenging to detect and attribute thereby causing non-repudiation attack.

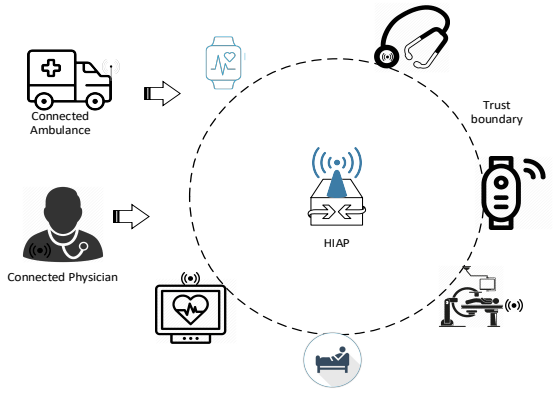


Figure 1: Typical IoT Use Case.

Already, cybercriminals have leveraged the inherent vulnerabilities in IoT engines to cause major disruptions, especially the Distributed Denial of Service (DDoS) attacks, which exploited Domain Name System (DNS) requests [31]. With the estimated 20 billion connected physical objects by 2020, and the explosion of industrial internet of things, recruiting thousands of connected devices to cause DDoS may be trivial. The foregoing typically suggests that a trusted party authorized to gain access to an IoT engine, can misuse it by employing the device to carry out other functions than originally programmed. For instance, GDPR[32] prescribes that personal data be used only for the initially stated purposes [13]. This provision makes privacy a contractual responsibility that must be respected by transacting IoT entities. Similarly, trust relationship is the requirement that attempts to guarantee the expected behaviour i.e. the hope that an IoT entity will behave reciprocally and responsibly without impairment to the other party. Thus, in practice, this mutuality may be too difficult to achieve.

Potentially, IoT poses different set of threats and risks in diverse environments and contexts, which should be addressed dynamically and in perspective [4]. For instance, in healthcare scenario, a Physician may have the need to work in several hospitals, of which her digital trust is not provided by the same or single security domain. It implies that this kind of use case requires that a high level of trust be established, privacy to be guaranteed, and confidentiality to be kept as well as the assurance of accountability and non-repudiation [33]. In healthcare environment, diagnosis, monitoring and assessment of patients may require significant number of devices interconnected by Heterogeneous IoT Access Point (HIAP) to collaborate and cooperate to solve patient's problems. In the same vein, the Physician's IoTs without previous trust relationship, may be required to interact with other IoTs within the environment. In this scenario, for convenience sake, the Physician IoTs should discover and connect automatically to the same HIAP or gateway without recourse to manual configuration. Another simple real-world use case is a connected ambulance that brings a patient to a smart hospital environment, under the characteristics of the mission (or emergency), the ambulance should be able to discover and automatically connect to relevant devices to accomplish its mission without manual configurations.

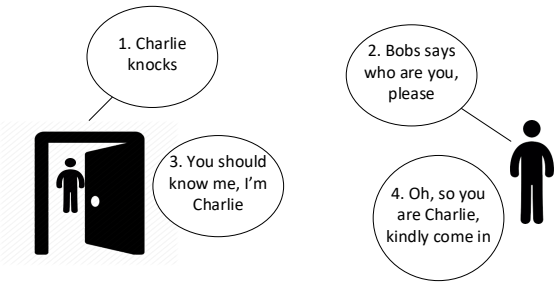


Figure 2: Trust Dialogue between Bob and Charlie.

Figure 1 depicts a typical smart healthcare environment. In many IoT systems, the manufacturers can provide a sort of security abstraction, which other security features can be derived, such features cannot by default solve application layer security that is usually contextual.

Like other computing devices, inbuilt security at abstraction layer cannot address application layer security and privacy out of the box, especially in distributed environments. In practical sense, security, privacy, and trust are not static security requirements. The implication is that these issues must be treated in context and instantaneously too. Moreover, IoT systems are probably going to expose services through Application Programmable Interface (API), this further reinforces the requirement for dynamic security, privacy and safety solutions that should be configurable[2]. To further provide insight to underlying concepts, we examine trust, privacy and confidentiality individually, and in perspective.

### *3.1. Trust Context*

Building digital trust in typical IoT in distributed environment raises fresh security issues. In digital space, building trustworthiness is vital, and can then be built between physical

objects, physical objects and people, physical objects and systems as well as systems. Thus, trust is a critical factor in distributed IoT environments that must be examined holistically. Theoretically, a simple trust dialogue between Charlie and Bob can be used to demonstrate generally, the subtlety of trust as a concept, shown in Figure 2:

Step 1: Charlie arrives at Bob's door and knocks;
Step 2: Bob says 'who are you, please?'
Step 3: Charlie answered, 'you should know me, I'm Charlie';
Step 4: Bob says "oh, so you are Charlie, kindly come in. In this case Bob allowed Charlie because he seems to recognize the voice of Charlie and anticipated to see him.

Examining this simple trust dialogue, there is a potential that Bob can open the door and see an imposter (who imitated Charlie's voice) instead of Charlie. This simplistic example, can be the basis to further discuss three important variables associated with trust namely: behaviour, reputation and expectations. Bob has merely trusted the statement based on known reputation and behaviour of Charlie with the anticipation that he will remain trustworthy. This modest example suggests there is inherent risk factors in the general concept of trust, thereby buttressing the point that current trust models provided by Public Key Infrastructure (PKI) are sufficient to guarantee trust in IoT environments. It further underscores the fact that providing security and safety features in IoT distributed systems require a sort of arrangement that gives the communicating parties to gradually establish more trust based on other attributes beyond PKI provisions.

In literature [34][23][35], digital trust is well researched, and provides the mechanism to verify and validate trust relationships, privileges, claims, identity attributes and information, etc.; giving the identity consuming party the opportunity whether to rely on the real-time assertions of proving party or not, based on the extended properties defined in the rule constraints.

### *3.2. Direct vs Indirect Trust*

Traditionally, digital trust is simply based on either direct or indirect (or transitive) trust relationships. In a typical IoT system, access to resources can be granted based on verification and validation of pre-existing trust relationships that authenticates a party requesting a service. Generally, this can be referred to as a direct trust, a form of shared secret, such as username/password pair or digital certificates, etc.; which is usually created offline between parties prior to communications as depicted in Figure 3(a). Figure 3(b) illustrates the concept of indirect trust whereby a service provider requires to verify and validate the assertions made by a party requesting service but there is no existing digital trust relationship between them. Thus, for a secure conversation, a trusted intermediary must prevail to vouch for the requesting party in a manner that a relying party can trust its assertions. Such examples as practiced today include signing into other third party online applications using Facebook or Twitter accounts.

In highly sensitive and safety critical IoT applications, simple trust models as described above is flawed substantially, which can easily be fooled by malicious parties. Based on the analysis already presented, different application contexts in distributed IoT environments, will require full-proof digital trust built gradually by reciprocated negotiation of verifiable attributes to assure security, privacy and safety.

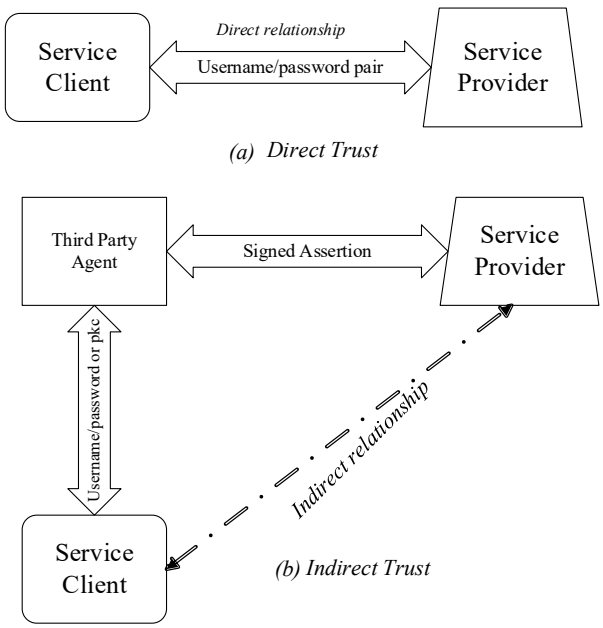


Figure 3: Classical Trust Models

### *3.3. Privacy and Confidentiality Context*

In many instances, privacy and confidentiality still remain a misunderstood concepts. It is not surprising as the terms are closely related. Conversely, in distributed application environments, where two or more actors are involved, privacy and confidentiality operationally are difficult to guarantee. For example, during access control phase, data of privacy value may be shared between these actors i.e. from requesting party's domain to the relying party, yet this privacy data may be disclosed by an intermediary party of another security domain. Data is fluid, and once shared with a third party, exercising full control thereafter becomes uncertain. While confidentiality can obviously be addressed by access restriction and/or encryption, privacy is subjective to trust expectations. So, it can be inferred that confidentiality is a means to ensure privacy protection especially when data is at rest but once the same data is passed unto a third party, then privacy may be eroded.

It is certain that personally identifiable information shared during transactions can be stored by either parties, to which the collector purportedly proclaims controls on behalf of the data owner. This raises privacy concerns, the data subject may lose track of the parties holding its data, and has no option but to rely on the facts of promise statements that the information will be given adequate privacy safeguards and protection. However, the new European Union General Data Protection Regulation (GDPR) has altered data privacy protection[13][36]. In the same wise, it may seem obviously that GDPR legal rules may have put stringent proscriptions but monitoring compliance and conformance is still operationally, a challenging task. Consequently, it suggests that in real-time, managing identity and access management, requires interacting parties to ensure that vouching for trustworthiness is cryptographically signed.

Above, entails that trust, privacy and confidentiality are strongly related and require a homogenous infrastructure to address them concurrently. To this extent, important questions can be raised to stimulate design assessment as follows:

(i) How can transaction entities account for their actions when privacy attributes are compromised or breached?
(ii) What are the technical mechanisms that can monitor how privacy data are accessed, shared and processed?
(iii) What is the assurance that a party can keep privacy promises made to another party, support and safeguard proportionately by suitable operational means?
(iv) Is there a technical mechanism to guarantee that transfer and processing of privacy information conforms to relevant standards and regulations, and its subsequent processing by second level third party?
(iv) What are the mechanisms to handle conflicts and risks? Is there a valid channel to handle and resolve conflicts that supports strong digital evidence?
(v) How can the liable parties be determined in multifaceted data breach involving several actors?
(vi) Is there any difficult-to-repudiate digital evidence that is admissible in courts of law to support assertions in an event of disagreement?

Imperatively, these questions can form open issues that challenges the research community and the need to find optimal solutions to address complex security, privacy and safety posture of IoT threat and risk landscapes, especially in the wake of increasing value of data [36][32]. Furthermore, it is an acknowledged fact that technology alone cannot answer all of the questions hypothesized above. As a consequence, it is remarkable to state that suitable governance, regulation and compliance, conflict resolution and assurance mechanisms, are vital inputs, which buttress the point that there is a strong interplay between technology, policy and law in solving privacy equations.

Notwithstanding, robust technical infrastructure has significant role in responding to the above named issues. Technically speaking therefore, dealing with real-time security, privacy and safety of connected devices operationally, require a flexible and distributed infrastructure that supports configurable policy constructs to manage IoT risks based on informed and preferred decisions.

## 4. Distributed Access Control Infrastructure

To design applicable access control infrastructure for IoT in distributed systems requires thorough examination of the various actors in a typical IoT conversations. As illustrated in Figure 4, there are likely to be multiple actors from different security domains that can interoperate in classical IoT service deployments. This is assumed on the ground that one security provider may be unsuitable for identity and access control to authenticate and validate security assertions that can be trusted across some high profile IoT distributed environments [12].

For instance, access to IoT systems in classical medical environment may require personal attribute of Medical Consultants from the Medical Council as well as a referrer attributes from a City Council as the basis to share or disclose resources. Equally, in a smart city, a rule requirement may entail that for vehicles to interact with city cameras for example, the vehicle license plate number as well as insurance certificate may need to be authenticated before access is allowed to protected resources. In this typical case, the attribute providers may unlikely be part of a single security domain. It implies that in distributed application scenarios, IoT access requires a robust and scalable infrastructure to treat security, privacy, and safety dynamically and in trusted fashion.

Figure 4 clearly illustrates conceptual view of access control entities in distributed environments. It shows entities and the various responsibilities as well as data flows. It is widely acknowledged that IoT is resource constrained for now; buttressing the fact that process consuming access control operations such as evaluation of access control policies may not be executed within IoT system. As such, light weight access control operations e.g. such as enforcement of decisions can be carried out in IoT systems, while other functions be delegated to trusted external parties.

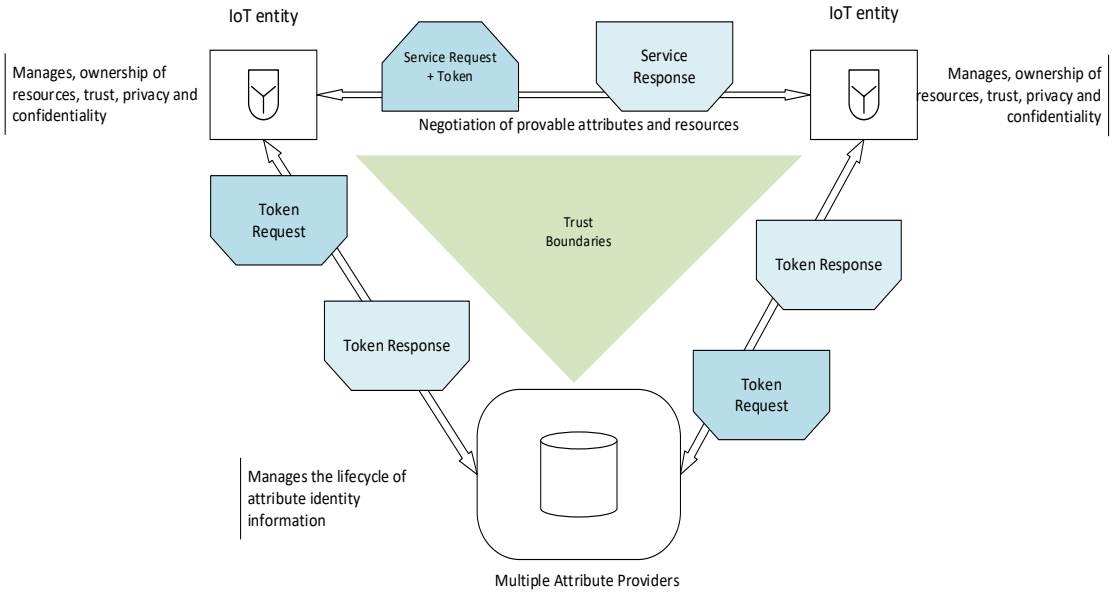


Figure 4: Conceptual View of Access Control Entities in a Distributed Environment.

*4.1. Distributed Access Control Infrastructure for IoT*

Figure 5 depicts Distributed Access Control Infrastructure that integrates components of FIM, Identity/Attribute Authority (IAA), and Obligation of Trust (OoT). The infrastructure components are loosely coupled in a distributed manner to allow interoperability and flexibility in deployment due to resource constrained IoT environment. The infrastructure consists of three logical subunits grouped according to areas or separation of concerns. The gatekeeper is tightly coupled to IoT application stack, which comprises Context Handler (CH) and Policy Enforcement Point (PEP) components of XACML. These components can programmatically be part of IoT system through its web service interface. The CH formulates or interprets specific application context data in a required format during conversations. Similarly, the PEP engine is responsible for the enforcement of access control decisions arriving at the gatekeeper after interpretation by CH. The Policy Decision Point (PDP) and Policy Information Point (PIP), still component of XACML provides decision point where serious policy *Matching Algorithms* are implemented. The Identity/Attribute Provider (I/AAP), which is derived from the concept of FIM supplies trusted attributes of entities to facilitate

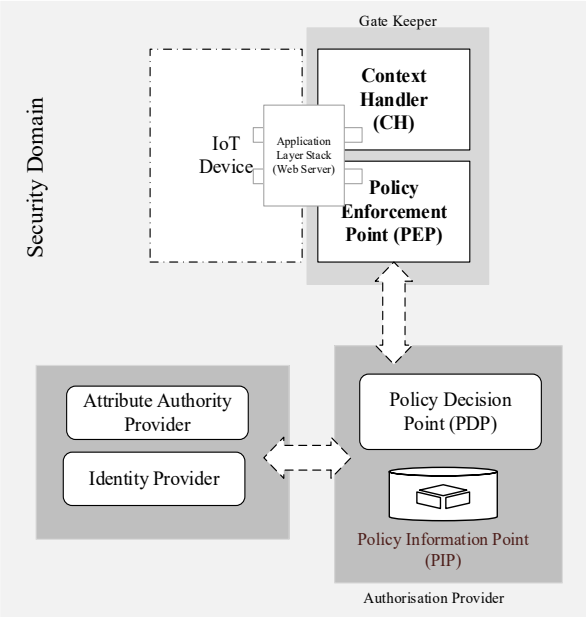


Figure 5: Distributed Access Control Infrastructure.

decision making by PDP. These subunits can then be hosted anywhere in the cloud to provide identity and access control functions. This infrastructural arrangement clearly shows the importance of IoT device belonging to a security domain where there is prevailing trust relationship with the authorization service for the solution to be feasible.

*4.2. SMAL OoT Protocol*

Figure 6 illustrates a protocol sketch between IoT entities in distributed systems, a way to mutually interexchange SAML OoT Assertion messages in order to decide whether resources can be shared either way [3].

The sequence of interactions are explained in the following steps:

1) A classical smart vehicle (SV) arriving a city sends a service request to Smart City Systems (SCS).
2) The request is intercepted by SCS Security gate keeper (CH/PEP), which constructs and sends SAML OoT containing Notification of Obligation (NoB) context.
3) The SV gate keeper intercepts, constructs and responds with its SAML OoT that contains its NoB.
4) The SCS CH constructs another SAML OoT that contains both NoBs and sends to its PDP for processing and decision.
5) The SCS's authorization engine based on the policy attributes sends SMAL OoT message to SV's IdP/AA requesting verification of identity/attributes of SV.
6) The SV's IdP/AA sends a corresponding SAML OoT *Response* message containing signed identity/attributes requested or makes a fresh request to the sending party (5 & 6 can iterate number of times depending on the trust negotiation configuration).
7) The SCS's authorization engine using the policy sets (NoBs) and based on 6 response, performs the *Matching Algorithm* to determine access decision.
8) The SCS sends SAML OoT *Response Message* that contains Signed Acceptance of Obligations (SAO) based on 7.
9) The SV's sends corresponding SAML OoT message that contains its SAO to SCS.
10) Then, SCS sends the requested resources to SV.

Note: Usually, direct trust can be the basis to initiate the negotiation, which usually, is a form of simple authentication; but not illustrated in the diagram.

*4.3. Obligation of Trust Policy Architecture*

Technically speaking, IoT in distributed setting is operationally complex and sophisticated, especially in interconnected and integrated application environments where applications talk to applications. To mutually treat trust, confidentiality and privacy, requires a configurable policy set that is robust and scalable. In this context, a policy construct that provides *Requirements* element and *Capabilities* element that permit each party to expressively and granularly describe its obligations and expectations is presented. Conversely, for IoT transaction parties to collaborate together in real-time, they can mutually express and interexchange the policy constructs containing *Requirements* and *Capabilities* in order to treat trust, confidentiality and privacy concurrently as illustrated in Figure 7. As demonstrated, party A's *Requirements* must match with party B's *Capabilities*, and similarly, party B's *Requirements* must match party A's *Capabilities* in a typical access request evaluation. This mutual evaluation gives each party, using granular expressive rules, the preference to decide and balance the sharing of resources in comparison to their mutual benefits. This construct when combined with *Digital Signature* solves confidentiality, integrity, authenticity and non-repudiation, thereby meeting basic security goals in a typical secure transaction.

In summary:

i. *Requirements* element is used to express a party's obligations (or commitments), it would expect another party requesting for a resource to fulfil before such a resource can be made available;

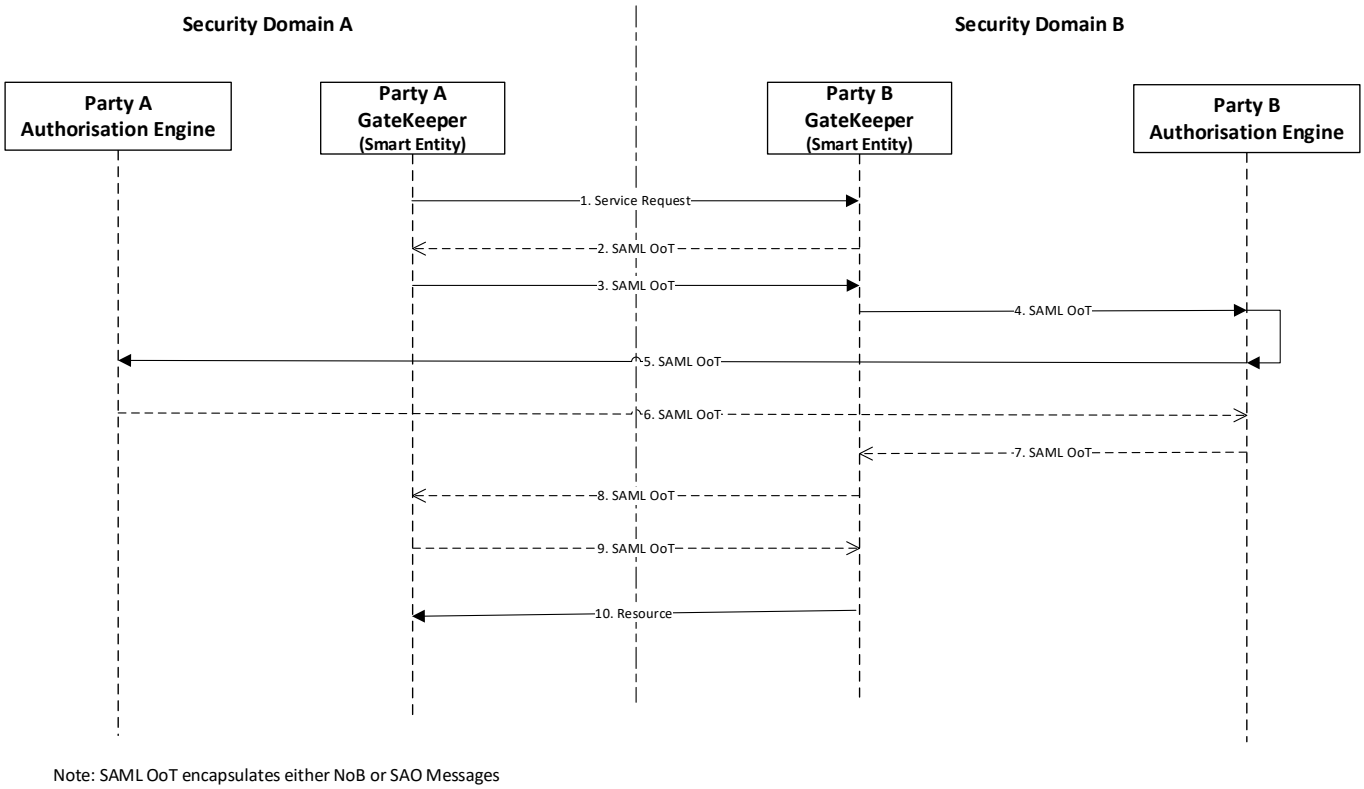


Figure 6: Access Control Conversations between Entities in Distributed Systems.

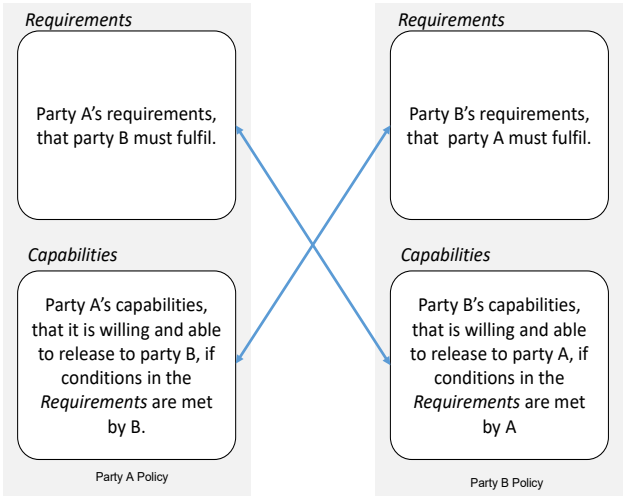


Figure 7: Obligation of Trust Policy Architecture

ii. *Capabilities* is used to express the competences (or services or features) a party is prepared to make available to another party, provided conditions expressed in its *Requirements* section are fulfilled. Thus, *Requirements* and *Capabilities* represent a policy architecture that two or more cooperating parties can leverage to assure trustworthiness, privacy and confidentiality concurrently.

The significant advantages of this policy construct include as follows:

i. It is a derivative of XAMCL and SAML standards, making it not too difficult to implement the *Matching Algorithms* and *Messaging* constructs;
ii. It is flexible to fit into any application context and has the ability to scale proportionately;
iii. It is extensible.

## 5. Discussions

The infrastructure presented here uses industry standards such as XACML, SAML, and frameworks including FIM, OoT for distributed access control in IoT environments. The infrastructural subunits are modular and distributed in manner adaptable to use cases where IoT computing resource are constrained. By design, it is expected that for an IoT entity to wade off application layer access intrusions, the gate keeper deny all access request by default. Consequently, to gain access to IoT resources depends on the evaluation of trusted assertion from a corresponding authorization service based on the outcome of *Matching Algorithms* by the PDP using the Policy Sets.

In implementation, there are two ways SAO can be constructed: firstly, the SAO can encapsulate digitally signed *Requirements* and *Capabilities* of a party. This signifies that this asserting party is willing and capable of providing the *Capabilities* if and only if the relying party meets the rules described in its *Requirements*. Secondly, in alternative, the SAO can comprise digitally signed *Capabilities* of the asserting party and the *Capabilities* of the relying party. In this case, it shows that the asserting party agrees to release the *Capabilities* provided the

relying party can reciprocate by releasing its own *Capabilities*.

In scenarios where incremental building of trustworthiness is required, more than one attribute would be required in the rule expressions in such manner that one of the *Subject Descriptors* of the policy indicates the initial attribute to start the first degree trust negotiation as may be required by the parties. Additionally, it can be assumed that parties may not be willing to disclose attributes of privacy value at the first round of the negotiation. In this regard, the policy specification should be such attributes required to build trust are arranged in order of less sensitive to high sensitive attributes. Alternatively, d*irect trust* between an IoT entity and its local IdP/AA, can be the basis for starting trust negotiation. The assumption here is that initial information provided by a party is insufficient to breach its privacy or undermine the confidentiality of the protected resources. This initial phase, in theory, is sufficient to counter any attempt by a malicious party to conduct probing attacks[23], usually related with trust negotiations. In this, it is further supposed that if the conversation parties decide to withdraw at the initial stage of the trust negotiation phase, their risks exposure can be significantly reduced. Moreover, if any of the parties is a hostile party, then this early interaction should filter out the access request, and terminate the conversation.

Whereas the first degree of the trustworthiness as described above is inadequate to gain access to IoT services, the parties may provide other levels of trust, which can be specified in the policy construct to help each other reach their various goals. To make this negotiation phase privacy aware, an entity can simply sends its SAML OoT containing its security *Requirements* and *Capabilities* across to the other entity. The later party, uncertain whether the other party will conform to its security settings, cannot disclose sensitive information, but correspondingly respond with another SAML OoT that describes its competences and security requirements. This iterative process operationally initializes privacy trust building and interexchange of applicable attribute information in intuitive way, which can result to a number of iterations until both parties are willing to work together.

It is obvious that the prevailing scenarios above is no way a guarantee or assurance that the parties will conform to each other's privacy, so the SAO offers a strong practical protocol that ensures conversation parties generate and interexchange digitally signed difficult-to-repudiate documents containing contextual information that can be admissible in the courts of law.

## 6. Conclusion

The infrastructure presented here introduces a powerful approach to identity and access management in distributed IoT environments in trust negotiation fashion. It has shown how malicious party's effort to intrude into an IoT system can be thwarted in real-time by gradual and bilateral negotiation to establish trust first before disclosure of protected resources in either direction. Privacy protection and trustworthiness, are behavioural, and possess obligatory expectations, it then implies that privacy and digital trust require a degree of assurance more than traditional security measures can provide. Our infrastructure has addressed security, privacy and safety in situations whereby IoT entities have to solve problems across multiple domains in more trustworthy, adaptive and secure manner. Equally, our approach allows both parties in conversation to mutually address their security, privacy and safety concerns as opposed to one-way unilateral protection mostly used by the party providing services.

Moreover, we have presented a novel infrastructure with distributed access control components in a fashion that access control Policy Decision Points (PDP), Identity/Attribute Authority (IAA) providers can be delegated to external trusted parties while the constrained IoT system handles context and Policy Enforcement Point (PEP).

Furthermore, by allowing parties to express their access rules and services in *Capabilities* and *Requirements* policy elements, a fine-grained access decisions can improve security and safety. Besides, addressing trust, privacy and confidentiality in a mutual way, our infrastructure provides accountability and conflict resolution approach, which are vital factors for typical IoT distributed deployments.

## Conflict of Interest

The authors hereby declare no conflict of interest.

## References


[1] U.M Mbanaso, G.A Chukwudebe, B. Bamidele "Holistic Security Architecture for IoT Technologies," in *13th International Conference on Electronics, Computer and Computation (ICECCO)*, 2017, pp. 11–16.

[2] U.M Mbanaso, G.A Chukwudebe "Requirement Analysis of IoT Security in Distributed Systems," 2017.

[3] U. M. Mbanaso, G. S. Cooper, D. Chadwick, and A. Anderson, "Obligations of trust for privacy and confidentiality in distributed transactions," *Internet Res.*, vol. 19, no. 2, pp. 153–173, 2009.

[4] U. M. Mbanaso, G. S. Cooper, D. W. Chadwick, and S. Proctor, "Privacy preserving trust authorization framework using XACML," *Proc. - WoWMoM 2006 2006 Int. Symp. a World Wireless, Mob. Multimed. Networks*, vol. 2006, pp. 673–678, 2006.

[5] R. Ross, M. McEvilley, and J. Carrier Oren, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," vol. 1, 2016.

[6] E. Number and H. Manufacturing, "Privacy and data protection."

[7] U. M. Mbanaso, G. S. Cooper, D. Chadwick, and A. Anderson, "Obligations for Privacy and Confidentiality in Distributed Transactions," *Ifip Int. Fed. Inf. Process.*, pp. 69–81, 2007.

[8] T. Ryutov, L. Zhou, C. Neuman, T. Leithead, and K. E. Seamons, "Adaptive trust negotiation and access control," *Symp. Access Control Model. Technol.*, p. 139, 2005.

[9] H. Gao, J. Yan, and Y. Mu, "Dynamic Trust Model for Federated Identity Management," *Netw. Syst. Secur. (NSS), 2010 4th Int. Conf.*, vol. 2010, pp. 55–61, 2010.

[10] A. Bhargav-Spantzel, A. Squicciarini, and E. Bertino, "Integrating Federated Digital Identity Management and Trust Negotiations," *CERIAS Tech Rep. 2005-46*, pp. 1–15, 2005.

[11] J. G. Alessandro Acquisti, "Privacy and Rationality in Individual Decision Making," *IEEE Secur. Priv.*, vol. 3, pp. 26–33, 2005.

[12] Information Commissioner's Office, "Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now," *Iso*, p. 11, 2016.

[13] Information Commissioner's Office, "Overview of the General Data Protection Regulation (GDPR)," p. 43, 2017.

[14] C. Weyrich, Michael und Ebert, "Reference Architectures for the Internet of Things," 2016.

[15] P. Fremantle, "A reference architecture for the internet of things," *WSO2 White Pap.*, vol. 0, p. 21, 2014.

[16] Symantec, "An Internet of Things Reference Architecture," *Symantec White Pap.*, pp. 1–22, 2016.

[17] K. E. Skouby and P. Lynggaard, "Smart home and smart city solutions enabled by 5G, IoT, AAI and CoT services," *Proc. 2014 Int. Conf. Contemp. Comput. Informatics, IC3I 2014*, pp. 874–878, 2014.

[18] A. Torkaman and M. A. Seyyedi, "Analyzing IoT Reference Architecture Models," *Int. J. Comput. Sci. Softw. Eng. ISSN*, vol. 5, no. 8, pp. 2409–4285, 2016.

[19] S. V. Nath, "IoT architecture," *Internet Things Data Anal. Handb.*, pp. 239–249, 2017.

[20] D. Chadwick, G. Inman, and N. Klingenstein, "Authorisation using Attributes from Multiple Authorities – A Study of Requirements," p. 4.
[21] B. E. Bhargav-Spantzel Abhilasha, Squicciarini Anna Cinzia, "Identity Management Concepts Technologies Systems," *IEEE Secur. Priv.*, vol. 5, no. 2, pp. 55–63, 207AD.
[22] OpenID, "OpenID Decentralized Authentication," 2017. [Online]. Available: https://openid.net/.
[23] K. E. Seamons Winslett, M. & Yu, T., "Limiting the Disclosure of Access Control Policies during Automated Trust Negotiation," *New York Distrib. Syst. Secur. Symp.*, pp. 1–11, 2001.
[24] D. Chadwick, G. Zhao, S. Otenko, R. Laborde, L. Su, "Building a Modular Authorization Infrastructure," *Kent Acad. Repos.*, pp. 5–15, 2010.
[25] B. Parducci and H. Lockhart, "eXtensible Access Control Markup Language (XACML) Version 3.0," *OASIS Stand.*, no. January, pp. 1–154, 2013.
[26] L. S. V *et al.*, "Security and Privacy Considerations for the OASIS Security Assertion Markup," *Management*, no. August, pp. 1–33, 2004.
[27] V. Felmetsger, "Security Assertion Markup Language ( SAML ) SAML as OASIS Standard," 2006.
[28] U. M. Mbanaso, "Design of Obligation of Trust Protocol," no. May, pp. 19–20, 2008.
[29] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in smart cities: Safety, security and privacy," *J. Adv. Res.*, vol. 5, no. 4, 2014.
[30] OWASP, "Internet of Things Top Ten," 2017.
[31] Gartner, "Leading the IoT, Gartner Insights on How to Lead in a Connected World," *Gart. Res.*, pp. 1–29, 2017.
[32] Information Commissioner's Offfice, "Guide to the General Data Protection Regulation (GDPR)," p. 153, 2017.
[33] U. M. Mbanaso, "Privacy Preservation Architecture for Authorization Infrastructure."
[34] K. E. S. Tatyana Ryutov, Li Zhou, Clifford Neuman, Travis Leithead, "Adaptive trust negotiation and access control," 2005, pp. 139–146.
[35] U. M. Mbanaso, G. S. Cooper, D. Chadwick, and A. Anderson, "Obligations of trust for privacy and confidentiality in distributed transactions) "Obligations of trust for privacy and confidentiality in distributed transactions Obligations of trust for privacy and confidentiality in distributed transactions," *Obligations Trust Priv. confidentiality Distrib. Trans.*, vol. 19, no. 2, pp. 153–173, 2009.
[36] U.M. Mbanaso, Centre for Cyberspace, Nasarawa State University, "Personal Data Privacy and Security - Who , What , When , Why , Where and How ?," in *DIRISA National Research Data Workshop, Pretoria South Africa*, 2018, no. June, pp. 1–8.