Known Unknowns: Indeterminacy in Authentication in IoT

Mohammad Heydari,[1] Alexios Mylonas,[2] Vahid Heydari Fami Tafreshi,[3] Elhadj Benkhelifa,[4] Surjit Singh[5]

[1,2] *Cyber Security Research Group, Bournemouth University*

[3,4] *School of Computing and Digital Technologies, Staffordshire University*

[5] *Department of Computer Engineering, National Institute of Technology, Kurukshetra, India*

Abstract

The Internet of Things (IoT), comprising a plethora of heterogeneous devices, is an enabling technology that can improve the quality of our daily lives, for instance by measuring parameters from the environment (e.g., humidity, temperature, weather, energy consumption, traffic, and others) or our bodies (e.g., health data). However, as with any technology, IoT has introduced a number of security and privacy challenges. Indeed, IoT devices create, process, transfer and store data, which are often sensitive, and which must be protected from unauthorized access. Similarly, the infrastructure that links with IoT, as well as the IoT devices themselves, is an asset that needs to be protected. The focus of this work is examining authentication in IoT. In particular, in this work we conducted a state-of-the-art review of the access control models that have been proposed, including both traditional access control models and emerging models that have recently been proposed and are tailored for IoT. We identified that the existing models cannot cope with indeterminacy, an inherent characteristic of IoT, which hinders authentication decisions. In this context, we studied the two known components of indeterminacy, i.e., uncertainty and ambiguity, and proposed a new model that handles indeterminacy in authentication in IoT environments.

Index Terms – Internet of Things, Authentication, Uncertainty, Ambiguity, Access Control

I. INTRODUCTION

Today, IoT, with more than 20 billion connected devices, introduces new security and privacy concerns. IoT is scaling up horizontally by expanding forms of data communication ranging from human-to-machine to machine-to-machine networks. It is also growing vertically by extending the capacity of resources and integrating more and more platforms and networks to form a heterogeneous environment. Most of the known IoT challenges have been investigated in areas such as smart cities, smart grids and e-health [1], [2], [3]. Among the challenges studied in the literature, access control was introduced as an open challenge that needs more investigation [4]. This is because governing access to big data produced by billions of smart devices needs a resilient, robust and real-time access control method. Furthermore, a number of IoT's inherent characteristics, such as scalability, heterogeneity, dynamism and resource sharing, amplify the security concerns related to access control. Scalability speeds up the velocity of data produced by Internet-enabled entities and similarly increases the variety of data sources that together leads to an increase in volume of the data produced. Integrating different platforms, networks and technologies such as WSN, RFID and GSM into a heterogeneous environment poses new concerns in terms of interoperability for governing access.

In such a heterogeneous environment, not only is achieving a secure and seamless integration of different platforms a challenge, but data access control also becomes more cumbersome. *Dynamism* in IoT stems from the need for real-time access to interconnected things in which interactions require fast responses at suitable times. For this purpose, access control and any context-aware services are directly influenced. Resource sharing in IoT improves performance with minimum investment. However, it comes with the risk of insider threats and permission misuses. Data communication loss in the event of a network or device failure is inevitable, and this might render the data in IoT inaccurate or incomplete. The incompleteness and imprecision inherent in the above-mentioned contexts can hinder precise access control decisions.

The main focus of this work is on "indeterminacy" as a new and unseen obstacle to securing IoT. It has a direct impact on the authentication phase of access control. Indeterminacy plays a crucial role in IoT when there is a need to make an informed access decisions based on incomplete or inaccurate information. In other words, indeterminacy appears when the access control mechanism needs to decide whether or not an entity is authenticated on the basis of with insufficient or inaccurate information, If indeterminacy is considered in this case, then this can lead to more precise decision-making when access is granted to different IoT devices and parties.

Some of the aforementioned characteristics of IoT complicate indeterminacy in data access scenarios. In particular, dynamism may exaggerate challenges in indeterminate access scenarios. In order to handle dynamism in access control, real-time activities and changes in the system need to be monitored. The inability to track these changes leads to a state of access decision-making that we describe as an "indeterminate state". Moreover, delay and latency caused by network deliveries in a heterogeneous environment may cause the same issue – that is, insufficient information to make informed access decisions.

The main aim of this work is to survey access control in IoT with a particular focus on indeterminacy. The rest of this paper is organized as follows: Section 2 discusses access control in IoT and presents the suitability of current access control models, protocols, standards and language for IoT. The concept of indeterminacy in authentication will be introduced in Section 3. The proposed model to handle indeterminacy in authentication will be presented in Section 4. The paper concludes in Section 5.

II. Access Control in IoT

Access control is a mechanism that determines the precise level of access to system resources based on a policy. It consists of authentication, authorization and auditing functions. The focus of this work is on authentication. In relation to access control, a number of characteristics have been discussed in the literature, such as delegation, revocation, granularity, flexibility, scalability, low

weight, heterogeneity and context-awareness [5]. According to the inherent characteristics of IoT, an access control system can be evaluated by the following criteria [6]:

1. **Scalability:** The authentication method must be scalable in three different dimensions: *a) subject/object (entities):* the performance (in terms of processing time or workload) of a scalable authentication method is not increased by the number of entities; b) *policy rules:* if the number of access policy rules increases it does not result in overhead; and *c) extensibility:* the ability of the structure to expand is important for the authentication method in the context of a heterogeneous environment such as IoT. Extensibility can be achieved through a decentralized architecture to cover different subsystems and domains.
2. **Heterogeneity/Interoperability:** An IoT-based authentication method must be applicable to different domains and platforms to cope with the heterogeneity of the IoT environment. In order to be thus applicable, the method must consider dependencies among entities and their workflows. Governing the authentication process in such an environment can be more challenging than in the traditional environment because of these dependencies.
3. **Dynamism:** If the values of the environmental attributes change while the subject is being authenticated then the granted access must be revoked. IoT needs a dynamic authentication method because of the rapid changes that can happen to the values of contextual attributes in such an environment.
4. **Context-Awareness:** In order to bring flexibility into access decisions, an authentication method must consider changes in contextual attributes to make more precise access decisions. It should be able to monitor the subject, object and environmental changes if these changes have impacts on the access decision.

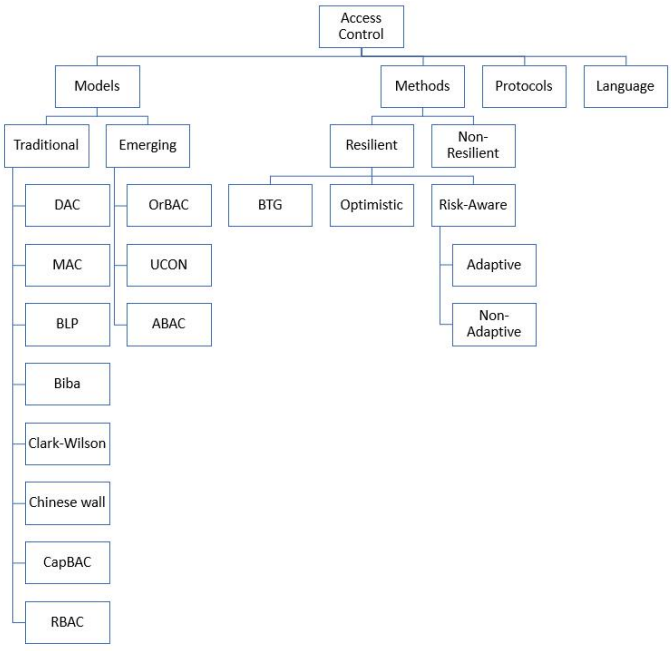

Figure 1: A classification of access control models, methods, protocols and language

Figure 1 depicts the classification of access control models, methods, protocols and language. In the rest of this section, the building blocks of this classification are analyzed based on the above-mentioned criteria in order to investigate whether they are applicable to IoT.

A. Access Control Models

Several access control models have been proposed since Lampson's access matrix was introduced in the late 1960s. According to [7], Discretionary Access Control (DAC), Mandatory Access Control (MAC), Bell-LaPadula (BLP), Biba, Clark-Wilson, Chinese Wall, Capability-Based Access Control (CapBAC) and Role-Based Access Control (RBAC) have been classified as traditional access control models. We refer to Attribute-Based Access Control (ABAC), and other models such as Access Control Based on Usage Control (UCON) and Organizational-Based Access Control (OrBAC), as *emerging* access control models. According to the above-mentioned criteria for evaluating access control systems, neither traditional nor emerging access control systems are applicable to IoT. Table 1 shows the performance of the access control models against four evaluation criteria in detail [6].

Table 1: Evaluation of traditional and emerging access control models

Criteria / Models	Scalability			Heterogeneity Interoperability	Dynamism	Context-Awareness
	Entities	Policy rules	Extensibility			
DAC	-	-	✓	-	-	-
MAC	-	-	-	-	-	-
RBAC	✓	-	-	-	-	-
CapBAC	-	✓	-	-	-	-
ABAC	-	-	✓	✓	✓	✓
UCON	-	-	-	✓	-	✓
OrBAC	✓	✓	✓	-	-	-

Table 2 summarized a number of proposed access control models that are based on an extension of the models listed in Table 1. The proposed methods have tried to address the limitations of the reference models stated in Table 1. Jindou et al. [8] proposed an access control model based on RBAC for the Web of Things (WoT). This model gathers information from users' profiles on social media platforms such as Facebook to create access policies. This, however, opens up a new type of

trust and privacy challenges for all participants in the access control model. Barka et al. [9] integrated RBAC and WoT to build an access control model with a centralized architecture. Access decisions are made by the Access Control Decision Facility (ACDF) based on an RBAC policy. Because of its centralized structure, the model cannot cope with a distributed environment such as WoT. Jing Liu et al. [10] have adapted the RBAC model to IoT using the Elliptic Curve Cryptosystem (ECC). In this method, IoT devices should be registered to a nearby trustworthy access point or gateway (termed as a Registration Authority). Furthermore, the authentication protocol suggested in this method is based on OpenID protocol, so it cannot be adaptable to IoT. Finally, it is not clear how the method identifies roles and assigns them, and nor has the work considered how RBAC can be adapted in the context of IoT.

Waleed et al. [11] proposed an access control model based on ABAC that incorporates trust and privacy into access policy to make it reliable in a collaborative environment. This model supports the privacy of subjects by authorizing certain access requests so that the purposes of access for both the subject and the object are the same. The limitations of the method include the following: a) if the contextual parameters have changed during the access time, the access decision nonetheless remains the same, and b) the proposed approach cannot be applied to distributed architecture, including P2P platforms. Kaiwen et al. [12] proposed a hybrid access control model based on RBAC and ABAC that can resolve the large-scale dynamic problem of IoT users. This model pre-assigns roles for entities (nodes/users) based on their property expressions. The model also presents a property rule policy language and a solution to the conflict with the redundancy policy. The authors in [13] used the WeChat App to illustrate the feasibility of this model. This model simplifies the complexity of traditional ABAC in right allocation and policy management. However, it cannot deal with policy conflict or redundancy processing as the model still needs the administrator to manage roles and access policy. Harsha, S., et al. [14] proposed an access control method based on ABAC for use in healthcare. The focus of this work is on providing both multilevel controlled access delegation and on-demand attribute revocation. The authors in [14] suggested using assignment tokens and digital signatures to handle delegation and revocation. The complexity of using the token-based approach in conjunction with ABAC was not investigated by the authors. Furthermore, the structure of token distribution and the validation scheme was not tested against forged intra-domain authorities, which may issue fake attributes and tokens.

Guoping et al. [15] proposed a method based on the extension of UCON. This method governs access by evaluating the degree of trust in the subject against the degree of trust of the object and the environment. If the trust value of the subject is in the range of the determined threshold for the requested object, then the access will be granted. The authors showed that their model works theoretically, but it is unclear whether it can work in a real-world scenario. Anggorojati et al. [16] proposed an access delegation method based on the context-aware CapBAC and identification. In

this model, context information was added to CapBAC as a new dimension. This method has used the concept of the federation in the Web for IoT by mapping identity to "thing". Mahalle [17] proposed a novel method for authentication and access control based on the approach proposed by [18]. In this method, verification of communication is done via its capability access. In other words, if any entity wants to communicate with another entity, communication is established after verifying the capability of the requesting entity. The proposed model uses a public key approach and is compatible with the lightweight, mobile, distributed and computationally limited nature of IoT. In this work, scalability, granularity and delegation were introduced as the main advantages of this method but the computational overhead of applying the model was not examined. Moreover, the interoperability of the proposed method in a heterogeneous environment such as IoT is still recognized as an open challenge. Gusmeroli et al. [19] proposed another model based on CapBAC, which uses a centralized approach for governing access control. The bottleneck for this method is that the majority of IoT devices have constrained resources and the overhead of the proposed method was not studied in this work. Yeh et al. [20] proposed a CapBAC-oriented access control framework for the e-healthcare domain. This method supports both fine-grained access control and revocation. The execution time for the encryption algorithms included in this method was compared with similar work to show its efficiency in terms of computational complexity. Although the proposed approach was proved theoretically, no experiment was conducted to show its efficiency in practice.

Li et al. [21] proposed a method that permits a user in a domain (e.g., smart city, smart grid) to send a message to a sensor in a domain that uses identity-based cryptography. The most important characteristic of this method is that it supports communication between heterogeneous environments. Furthermore, authors in [21] showed that the computational cost of the sensor node in their method is reduced and energy consumption is consequently reduced. Patel et al. [22] proposed an energy-efficient access control method for IoT using elliptic-curve cryptography. The proposed method was evaluated using the AVISPA[1] tool against attacks such as man-in-the-middle, reply attack and DoS. Even though the proposed method mitigated all these attacks successfully, one limitation of this work is that the method's efficiency was not considered. Ouaddah et al. [23] proposed a model based on an extension of OrBAC, which focuses on low power consumption. To meet this goal, part of the processing burden of PDP was transferred to end-point devices to make the centralized structure more flexible. However, the overhead of the proposed method in terms of computational complexity and energy consumption was not proven experimentally. Moreover, the interoperability of the proposed scheme has not been studied. Sciancalepore et al. [24] proposed an access control framework based on OAuth 2.0, which consists of a wireless sensor network, client, gateway and authorization server. The authorization server passes the access request to the resource owner and generates the access token for the subject to which the access is granted. One of the challenges in

[1] Available at http://www.avispa-project.org

this method is that direct communication between entities (without the presence of a gateway) is not possible due to the role of the gateway. The following conclusions arise from the study of the literature:

- In the approaches designed as an extension of RBAC, scalabilty in IoT was studied. Morever, the interoperability issue was addressed through a Web-based interface (WoT).

- CapBAC-based approaches, even those using lightweight encryption algorithms (e.g., ECC), suffer from computational overhead in a scalable environment (e.g., cloud, IoT). Morever, applying certificate-based authentication brings new challenges in terms of certificate validation and management in a heterogeneous environment such as IoT. In other words, moving from one domain to another makes interoperability a major concern for certificate validation.

- Although ABAC-based approaches bring flexibility by considering contexual parameters, managing a number of attributes in a hybrid model using role assignment by RBAC or by using public-key encryption like Attribute-based Encryption (ABE) introduce overhead and interoperability issues in IoT.

Table 2: Analysis of proposed access control methods for IoT

Criteria / Method	Scalability			Heterogeneity Interoperability	Dynamism	Context-Awareness
	Entities	Policy rules	Extensibility			
[8]	✓	-	✓	-	-	✓
[9]	-	-	✓	-	-	✓
[10]	✓	-	✓	✓	-	-
[11]	✓	-	✓	-	✓	✓
[13], [12]	✓	✓	-	-	-	✓
[14]	-	-	-	-	✓	✓
[15]	-	-	✓	-	✓	✓
[16]	-	-	✓	-	-	✓
[17]	✓	-	✓	✓	-	-
[19]	-	-	-	-	-	✓
[20]	-	✓	-	-	✓	✓
[21]	✓	-	✓	✓	-	-
[22]	✓	-	-	-	-	-
[23]	✓	✓	✓	-	-	-
[24]	✓	-	✓	✓	-	-

B. Access Control Protocols and Standards

This subsection first introduces the most widely used access control standards and protocols, followed by a discussion of their applicability in IoT. In order to evaluate the protocols involved in access control the following criteria that are proposed in RFC 2989 and RFC 4962 are used:

1. Overhead: IoT devices are resource-constrained and thus any proposed access control protocol for IoT must be lightweight. To evaluate overhead, two different parameters are considered: *a) communication overhead*, which can be measured by the number of messages exchanged in a data access scenario per access request; and *b)* the *lightness of data exchange format*, which affects the amount of required control traffic per access. Increased overhead may result in increased power consumption. For this reason, some works have suggested using more efficient protocols than WiFi RF for communicating over IoT, such as LoRA [25]. Poursafar et al. [26] compared short-range and long-range enabling technologies involved in IoT. The writers presented a new classification for low-power wide-area networks which are introduced as an efficient and promising technology in IoT.
2. Security of data-in-transit: The confidentiality of credentials that are sent over the network should be ensured. Otherwise, the protocol is prone to breaches of confidentiality of (credential) data-in-transit.
3. Architecture: The structure of access control protocols can be centralized or decentralized. As services in the IoT environment are decentralized and distributed, centralized architecture for access control protocol does not work efficiently if the protocol is deployed in a heterogeneous environment.

The aforementioned criteria will be used to evaluate whether the following protocols fit IoT: i) *Open Authorization (OAuth)*,[2] an open protocol used to establish a secure authorization over the Web; ii) *OpenID*,[3] a Web-oriented single sign-on protocol that is widely used by well-known companies such as PayPal and Amazon; iii) *Security Assertion Markup Language (SAML)*, an XML-oriented and open protocol to exchange user authentication and authorization data among security domains; iv) *Remote Authentication Dial-in User Service (RADIUS)*,[4] an authentication network protocol that works in client/server network architecture to provide centralized access to networks (RFC 6929); v) *Lightweight Directory Access Protocol (LDAP)*,[5] which is a centralized and remote authentication network protocol used for authentication and authorization; and vi) *Kerberos*,[6] a network authentication protocol developed by MIT to provide access to university resources in the 1980s by authenticating clients to services in a distributed system. RADIUS, LDAP and Kerberos are widely

[2] https://oauth.net/
[3] http://openid.net/
[4] For more information, refer to RFC 2865 and RFC 6929.
[5] https://ldap.com/
[6] https://web.mit.edu/kerberos/

used in active directory and database access for access control.

In addition to the above de facto protocols, a number of studies have suggested new protocols. Braeken et al. [27] proposed a key agreement scheme based on symmetric encryption for IoT. The approach handles the verification of authentication for communications in which entities do not have prior trust relations.

These protocols suffer from vulnerabilities. Jurcut et al. [28] proposed an approach to detect exploitable vulnerabilities in authentication protocols. The proposed method used a novel logic-based technique to describe the circumstances under which a weakness in authentication protocols can be exploited.

A number of papers in the literature have proposed applying Blockchain technology to provide secure access in IoT. Zoubir Ourad et al. [29] suggested applying Ethereum smart contracts in IoT domains. The evaluation results indicated that the proposed solution benefits from a number of advantages including scalability, decentralization and integrity in comparison with OAuth 2.0.

Table 3 summarizes the comparative study between the above-mentioned authentication protocols based on the aggregated attributes that were discussed in the literature.

Table 3: Summary of widely deployed authentication protocols

Spec	OAuth	OpenID	SAML	RADIUS	LDAP	Kerberos
Authentication	No	Yes	Yes	Yes	Yes	Yes
Authorization	Yes	No	Yes	Yes	Yes	No
Communication Overhead	Low communication overhead due to the use of JSON format	Low communication overhead due to the use of JSON format	High overhead due to XML parsing	Low in terms of server processing overhead	Low communication overhead due to using ASN.1, which is lighter than JSON	It imposes overhead in terms of control traffic and KDC administration in a scalable environment
Architecture	Decentralized	Decentralized	Centralized	Centralized	Centralized	Centralized
Security of credential data in transit	Confidential	Confidential	Confidential	Only passwords are encrypted	Confidential	Username is sent in plain text, but passwords remain confidential

C. Access Control Language

Extensible Access Control Markup Language (XACML) is a de facto standard and language to express ABAC-based access control policies, which is based on XML and developed by OASIS.[7] It uses *policy language* to define access policies and *request/response language* to describe access request queries and responses. According to the findings of this research, XACML has the following advantages in modelling: i) XACML is a standard that has been reviewed by a wide community of experts and users; ii) it offers a comprehensive framework to build policies and provides an expressive language that supports a diverse collection of data types, functions and combining algorithms that can be easily extended; iii) XACML is sufficiently generic to be deployed in any environment – it makes policy management easier; and iv) it can be utilized in distributed contexts, which means that a policy can refer to other policies. In other words, XACML can combine results from different policies into a single decision.

D. Resilient Access Control Approaches

Traditional access control approaches operate based on a set of static policy rules that govern access. In these approaches, access is granted if the corresponding rules are fired. Each rule consists of parameters to handle a condition in the predicted access scenario. The values of these parameters should be available if the rule needs to be fired. In such a system, if some of the rule parameters are missing then the system cannot handle the access scenario. As discussed earlier, scalable and heterogeneous environments such as IoT consist of data access scenarios in which making access decisions (e.g., authentication) based on the available information is not feasible due to a lack of information. In such a non-resilient access control system, the output leads to the access request being rejected. Therefore, a new paradigm is needed to make precise access decisions based on incomplete information and bring resilience to access decision-making. This type of access control is called "resilient access control". Three paradigms have been proposed to achieve this goal [30], [31]: (i) Break-The-Glass (BTG) Access Control; (ii) Optimistic Access Control; and (iii) Risk-Aware Access Control (RAAC).

1. Break-The-Glass Access Control (BTG)

Ferreira [32] suggested BTG to allow access rule overrides. The aim of this model is to allow unanticipated access to be provided in unpredicted situations such as emergencies in e-healthcare

[7] https://www.oasis-open.org/

[27]. Scalability is the most important challenge of BTG because growing the number of access rules overriding the access means that governing and auditing become impossible [33].

2. Optimistic Access Control

Optimistic Access Control was proposed to provide access in emergency scenarios (e.g., e-healthcare) in which availability is needed more than confidentiality. The optimistic paradigm assumes that most access requests will be authentic, and it allows subjects to exceed their normal permissions. In such a system, adopting an extra control layer to protect the resources from misuse is a must. As with BTG, the lack of scalability in terms of access policy rules is the drawback of this paradigm [30].

3. Risk-Aware Access Control (RAAC)

RAAC was proposed to evaluate the risk of the access request to determine whether access to a resource should be granted [34]. RAAC includes the process of risk assessment, which is defined as the process of identifying, estimating and prioritizing risks to organizational assets and operations (NIST SP-800). It enables the resource owner to obtain a view of existing security risks and their impacts. Three taxonomies were proposed for risk assessment [35], [36]:

- The most recent taxonomy classifies risk assessment based on the level of analysis into three categories: i) *asset-driven*, in which the assessment starts by identifying and evaluating the assets; ii) *service-driven*, in which the services are identified first and then risks associated with these services are evaluated; and iii) *business-driven*, in which business goals and associated processes should be identified first and then the risks related to these business goals are assessed.
- Another taxonomy for risk assessment methods is based on risk measurement. Risk-measuring methods fall into two categories: i) *non-propagated*, where risk is measured regardless of its propagation impacts on the other risk parameters; and ii) *propagated*, where dependencies among the resources and their impacts on each other are taken into consideration to measure the risk.
- Risk-aware access control methods can be classified into two categories: non-adaptive RAAC and adaptive RAAC. Non-adaptive RAAC refers to the class of methods in which even when the values of risk factors changed the calculated risk value remains unchanged, and therefore non-adaptive RAAC is not sensitive to changes in the parameters involved in the access scenario. In contrast, the calculated risk value in adaptive RAAC may change because of changes in the parameters of

the risk factors. Therefore, tracking of activities and monitoring of situational parameters are vital in adaptive RAAC in order to reflect the changes and make the necessary change to granted access.

- In order to measure the value of the risk, in the literature a number of metrics are suggested, including object sensitivity, the severity of the requested action and the benefit of the access [37], [38]. Moreover, five different methods were suggested for calculating the total value of the risk, and these were discussed in [6]. These classes take into consideration different parameters such as the likelihood of incident, the likelihood of threat, and the impact of the threat or incident.

E. Finding on RAAC Approaches

There are a number of widely used standards and methodologies for risk assessment, such as NIST-SP800,[8] ISO/IEC 27005:2011[9] and IEC 62443-2-1.[10] Each describes a specific method for risk identification, evaluation, prioritization and mitigation. The adaptability of these risk assessment standards and methodologies in the IoT environment is controversial. Nurse et al. [39] argued that if IoT-related characteristics, such as scalability, heterogeneity and dynamism, are taken into consideration', the current risk assessment approaches are inadequate for IoT for the following reasons:

- *Limitation of periodic assessment for the IoT environment*: The current risk-based approaches are based on periodic assessment and therefore cannot identify and evaluate significant changes in a highly dynamic system such as IoT, where there is a high degree of variability in system scale, dynamism and coupling.
- *Lack of knowledge of IoT entities*: Most of the current risk assessment approaches are based on knowledge of assets, threats, attack probabilities and potential impacts of threats. However, achieving sufficient knowledge of these parameters in IoT is extremely challenging due to the scalable and dependable environment of IoT.
- *Interoperability and dependency challenges*: Current risk assessment approaches are unable to assess all the processes associated with the assets and the inter/intra-connections that allow them to couple and operate.

One of the big challenges for most existing RAAC methods is that they are manual [40]. Those RAAC methods that rely on a low degree of automation are not applicable in a scalable and heterogeneous environment such as IoT because the cost of the manual RAAC process in terms of time and money would be high and the whole process would be error-prone because of human intervention. Furthermore, existing RAAC approaches suffer from vulnerabilities that lead to social engineering attacks. Moreover, most of the proposed RAAC methods are based on assumptions that

[8] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
[9] https://www.iso.org/standard/56742.html
[10] https://webstore.iec.ch/publication/7030

affect their generalizability and make them domain-specific solutions rather than generic methods [41].

III. INDETERMINACY IN AUTHENTICATION

Indeterminacy has not received the attention that it deserves as a challenge in IoT, compared to other challenges that are well-studied in the relevant literature, such as scalability, heterogeneity, interoperability and dynamism [1], [2], [3], [42], [43]. However, as this work stresses, indeterminacy should be considered when making an access control decision in IoT. Otherwise, if the decision is based on deterministic rules regardless of the indeterminacy concept, this leads to a binary decision (Access/Deny), which does not fit in a dynamic environment such as IoT.

According to [44], there are at least two facets of indeterminacy: *uncertainty* and *ambiguity*. In the context of authentication, we consider that uncertainty is caused by a lack of information about the likelihood of an incident occurring. Also, ambiguity is caused by a lack of precision in the information required to make a decision. In the rest of this section, uncertainty and ambiguity in access control are discussed.

A. Uncertainty

Uncertainty is rooted in randomness. Randomness has traditionally been used to describe probabilistic events. The term uncertainty was coined by Knight in 1921 and appeared in Keynes's writings in 1936 [45]. Uncertainty refers to a situation in which it is not certain that an event will occur. Uncertainty is classified into three categories [46]:

i) *Aleatory uncertainty* concerns purely random events. Accurate prediction about random events is not achievable.

ii) *Epistemic uncertainty* describes events with unknown parameters and properties of their occurrence. Most of the uncertainty found in IoT belongs to this category.

iii) *Inconsistent uncertainty* refers to a situation in which the information available about the occurrence of an event is inconsistent. Gathering more information about the event leads to more conflicting testimonies.

Historically, the concept of uncertainty came from economics (e.g., risk management, stock market forecasting) and management (decision-making) into computer science and is used to describe situations in which prediction of future events is not possible. Learning how to handle uncertainty in all of these domains gives insight to decision-makers so they can prepare themselves to face

unpredicted scenarios. In order to handle uncertainty, five main theories have been proposed: i) probability theory; ii) information theory; iii) evidence theory [47]; iv) possibility theory [48]; and v) uncertainty theory [49].

We summarize below the strengths and limitations of these theories in handling uncertainty:

- Probability theory: Using subjective probability to model uncertainty is too narrow and leads to poor predictions, particularly in cases where aleatory uncertainty is mixed with epistemic uncertainty.
- Information theory: The performance of entropy analysis depends on the probabilistic model used. If a poor model has been used, the outcome of such an analysis will not be reliable.
- Evidence theory: This theory has the ability to aggregate multiple sources of uncertainty, so it works for inconsistent uncertainty. This theory has the same limitation as subjective probability theory in handling uncertainty when aleatory uncertainty is mixed with epistemic uncertainty.
- Possibility theory: Possibility theory uses fuzzy measures to represent uncertainty. It needs fewer arbitrary assumptions than probability theory. It makes more precise predictions than subjective probability. When using this theory, empirical information is not needed to make a prediction.
- Uncertainty theory: This is a relatively new theory in the field of uncertainty representation. It is suitable when too few samples are available, so this theory is the main competitor to possibility theory. The main difference between uncertainty theory and probability theory is that in probability theory the product probability measure is the product of the probability measures of the individual events, whereas in uncertainty theory the product uncertainty measure is the lowest of the uncertainty measures of the individual events.

Making accurate authentication decisions based on incomplete information brings flexibility into the access control domain. As a result, uncertainty in authentication needs to be defined. As we previously defined it [6], uncertainty in authentication can be defined as a state in which access decisions have to be made based on incomplete information. There are a number of domains in which such a resilient method can be applied, such as vehicle-to-vehicle communication (VANET), virtual organization (VO) in smart grids, and resource sharing (e.g., traffic information) in smart cities. Such uncertainty is measured by calculating the probability of whether authenticating a subject will result in a security incident. In the world of security, “risk” is the concept most similar to “uncertainty”. These two concepts have “the likelihood of event occurrence” in common. In order to handle the risk, the impact of the event in question needs to be considered as well. Moreover, risk leads to vulnerability, and assessment of the value of risk cannot be accomplished without evaluating vulnerabilities.

B. Ambiguity

One of the goals of this research was to identify the differences between uncertainty and ambiguity in authentication domains because these two concepts are used interchangeably in the literature [50], [51]. Consequently, the methods proposed to handle them are used interchangeably too. The term "ambiguity" was coined by Aristotle and referred to vagueness. Ambiguity is caused by imprecise information rather than incomplete information. Ambiguity in authentication is a state in which prediction of the trustworthiness of the subject fails as a result of imprecise or vague information. None of the theories mentioned that can be applied in uncertainty domains are able to give predictions on the future of the subject based on imprecise information. The sources of ambiguity may vary but the complexity of a system amplifies ambiguity [52]. As defined in [6], ambiguity in authentication is caused by a lack of precision in the available information about the subject who sends the authentication request. In order to handle ambiguity, it is necessary to determine to what extent the authentication system can trust the subject. In the attempt to do so, a number of attributes have been suggested in the literature, such as the profile history of the subject, and subject and object sensitivity. Applying soft computing methods such as fuzzy logic has been suggested to address the problem.

C. Proposed Methods to Handle Risk and Trust

A state-of-the-art review was conducted to answer the following research question: *Can resilient access control methods handle indeterminacy in IoT*? Table 4 summarizes the reviewed literature on resilient methods and indicates whether the existing approaches handle uncertainty and ambiguity. Bijon et al. [53] incorporated the concept of risk awareness into RBAC. In the proposed method the role of the subjects is assigned and activated based on the calculated risk. In this way, the total value for risk is calculated for all active roles assigned to the subject and if this value does not exceed the threshold the new role will be assigned.

Baracaldo et al. [54], [55] used trust and risk concepts in relation to RBAC to deal with insiders. In this method, the trust value is calculated for each user. Moreover, the risk value is calculated and assigned to each role by considering all direct and indirect access rights that are enabled by activating such a role. Furthermore, a role is activated if the user meets the minimum trust level required for that role. The value of the trust is determined based on the amount of risk exposed by activating the role. Dimmock et al. [56] proposed a method to enhance the RBAC with trust and risk. To meet this goal, trust and cost evaluation measures are added to the OASIS policy language. This method has introduced a risk evaluation expression language to calculate the risk based on the given values and make an access decision based on that calculation. Chen et al. [57] proposed an extension for the RBAC model to handle the risk by calculating the likelihood of the occurrence and mitigating the impact of the risk. The former was accomplished by evaluating the suitability of a given access policy

for a role and assessing the trustworthiness of the subjects. The latter was handled by obligating the users to avoid accepting any request with a risk value greater than the threshold.

Dos Santos et al. [58] proposed an RAAC approach based on the extension of ABAC for the cloud. Identifying the cloud federations for the subject and for the object is the major part of this method. If the cloud federations for the subject and for the object are the same then ABAC policy is applied, but if the federations are not the same then a risk assessment should be done for the subject to determine whether the overall risk for the subject is less than the threshold for granting access. Dos Santos et al. improved their approach [59] proposed in 2014 and enriched their method by applying RAAC not only for intra-cloud access decisions but also for inter-cloud access decisions. Ricardo et al. [60] proposed a risk-aware framework to enforce RAAC policies in the cloud. This work is based on the extension of XACML and aggregates various risk factors to calculate the final value of the risk. Risk itself is measured based on the impact that access can cause. The calculated value is compared to a threshold to make an access decision. Atlam et al. [61] developed an adaptive RAAC model for IoT. This model accepts real-time attributes including user context, resource sensitivity, action severity and risk history as inputs and estimates the overall risk value associated with each access request. A limitation of this work is that the authors did not validate their proposed model. Dorri N. et al. [62] proposed an access control framework for grid environments to address the misuse of resources in virtual organizations. This method offers both risk and trust analysis in authorization to assess the subject's actions. In order to measure the degree of trust for the users the proposed method uses feedback by applying the probabilistic approach. In addition to trust, the method assesses the risk based on the calculated value of trust. The proposed risk model predicts the likelihood of fulfilment of obligations. The proposed model was evaluated using simulation, which proved its scalability in terms of the number of entities, the number of policy rules and the degree of extensibility.

Table 4: Analysis of proposed resilient methods in the literature

Criteria / Method	Scalability			Heterogeneity Interoperability	Dynamism	Context-Awareness	Indeterminacy-Aware in Authentication	
	Entities	Policy rules	Extensibility				Uncertainty	Ambiguity
[53]	-	✓	-	-	✓	✓	-	-
[54], [55]	-	✓	-	-	✓	✓	-	-
[56]	-	✓	-	-	✓	✓	-	✓
[57]	✓	-	-	-	-	-	-	-
[58]	✓	✓	✓	✓	-	✓	✓	-
[59], [60]	✓	-	✓	✓	✓	✓	✓	-
[61]	✓	-	-	✓	✓	✓	✓	-
[62]	✓	✓	✓	✓	✓	✓	-	-

IV. PROPOSED MODEL

The model shown in Figure 2 is proposed to handle uncertainty and ambiguity in the authentication phase of the access control. The architecture of the model is based on XACML. The reasons for selecting XACML are that the proposed model is based on ABAC and works with contextual parameters as attributes. XACML is the standard (and language) for ABAC.

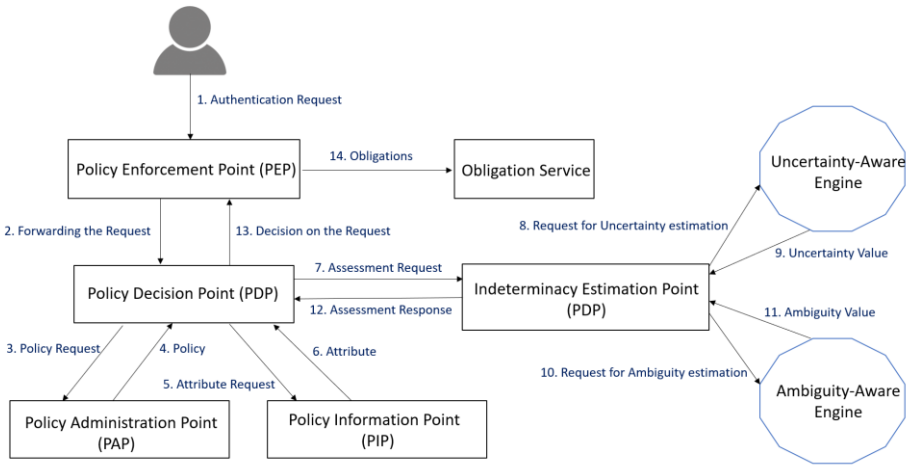

Figure 2: Proposed architecture for the indeterminacy-aware authentication model

As depicted in Figure 2, the data flow model is as follows:

1) A subject sends its authentication request to Policy Enforcement Point (PEP). PEP is the interface between the system and the subject to forward its request and return the decision in terms of obligations.

2) PEP sends the request to Policy Decision Point (PDP), which is responsible for gathering policy related to the specified resource from Policy Administration Point (PAP).

3) PDP requests policy from PAP.

4) PAP is responsible to provide requested policy to PDP.

5) PDP also requests subject, object and environment attributes related to the request from Policy Information Point (PIP).

6) PIP is responsible to gather attributes related to the request (subject, object, environment) and makes it available to PDP.

7) By having requested information, PDP sends the access request to Indeterminacy Estimation Point (IEP) for requesting both uncertainty-aware and ambiguity-aware engines to calculate the uncertainty and ambiguity values associated to the authentication request.

8) IEP sends request to uncertainty-aware engine to calculate the total value of the uncertainty associated with the authentication request.

9) Uncertainty engine return the calculated value to IEP.

10) IEP sends request to ambiguity-aware engine to calculate the ambiguity value (trust value) associated with the authentication request.

11) Ambiguity-aware engine returns the calculated value for the trust.

12) IEP calculates the value of indeterminacy based on the risk and trust values and sends it to PDP.

13) PDP makes final access decision using related policy and the value of indeterminacy which was provided by IEP. Then the decision will be forwarded to PEP.

14) PEP fulfills the obligations based on the authentication decision.

V. CONCLUSION

With the advent of IoT, the concept of resilient access control has gained considerable attention and pushed the limits of the conventional access control approaches. In this paper, we have analysed both traditional and emerging access control models in order to investigate whether they fit IoT. Our work indicates that the conventional models do not fit into IoT because of their lack of support for its inherent characteristics, such as scalability, heterogeneity and dynamism. Moreover, we have surveyed the resilient access control approaches to evaluate them against the criteria discussed, and our work has revealed the same drawbacks in terms of scalability, heterogeneity and dynamism. This work also focuses on "indeterminacy" as a challenge that is neglected in comparison with other challenges to access control in IoT. In this way, we have defined indeterminacy in authentication, which includes uncertainty and ambiguity in authentication. We have also surveyed the relevant literature that handles indeterminacy in authentication. Finally, we have proposed an indeterminacy-aware authentication model based on the extension of ABAC. Future research directions could include attempts to find a method to handle uncertainty based on the theories discussed.

REFERENCES

[1] Wei Zhou, Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved," *IEEE Internet of Things Journal*, pp. 1-11, 2018.

[2] ELISA BERTINO, KIM-KWANG RAYMOND CHOO, DIMITRIOS GEORGAKOPOLOUS, SURYA NEPAL, "Internet of Things (IoT): Smart and Secure Service Delivery," *ACM Transactions on Internet Technology,*, vol. 16, no. 4, pp. 22-29, 2016.

[3] Francesco Restuccia, Salvatore D'Oro and Tommaso Melodia, "Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking," *IEEE Internet of Things*, vol. 1, no. 1, p. IEEE Early Access Service, 2018.

[4] C. Zhang and R. Green, "Communication Security in Internet of Thing: Preventive measure and avoid DDoS attack over IoT network," in *IEEE Symposium on Communications & Networking*, 2015.

[5] Aafaf Ouaddah , Hajar Mousannif , Anas Abou Elkalam , Abdellah Ait Ouahman , "Access control in the Internet of Things: Big challenges and new opportunities," *Elsevier Computer Networks*, vol. 112, pp. 237-262, 2017.

[6] Mohammad Heydari, Alexios Mylonas, Vasilis Katos and Dimitris Gritzalis, "Towards Indeterminacy-Tolerant Access Control in IoT," in *Handbook of Big Data and IoT Security*, Springer, 2019.

[7] William Stallings, Lawrie Brown, "Access Control," in *Computer Security: Principles and Practice, 3rd Edition*, Pearson, 2015, pp. 113-154.

[8] Jia Jindou ; Qiu Xiaofeng ; Cheng Cheng, "Access Control Method for Web of Things Based on Role and SNS," in *IEEE 12th International Conference on Computer and Information Technology (CIT)*, 2012.

[9] E. Barka, S.S. Mathew, Y. Atif, "Securing the Web of Things with Role- Based Access Control," in *Springer International Conference on Codes, Cryptology, and Information Security*, 2015.

[10] Jing Liu ; Yang Xiao ; C.L. Philip Chen, "Authentication and Access Control in the Internet of Things," in *IEEE 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, 2012.

[11] Waleed W.Smaria Patrice Clemente Jean-Francois Lalande, "An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system," *Future Generation Computer Systems*, vol. 31, pp. 147-168, 2014.

[12] Sun KaiwenYin Lihua, "Attribute-Role-Based Hybrid Access Control in the Internet of Things," in *International Conference on Web Technologies and Applications. APWeb* , 2014.

[13] Sun Kaiwen Yin Lihua, "Attribute-Role-Based Hybrid Access Control in the Internet of Things," in *Web Technologies and Applications, Springer*, 2014.

[14] Harsha S.Gardiyawasam PussewalageVladimir A.Oleshchuk, "Attribute based access control scheme with controlled access delegation for collaborative E-health environments," *Elsevier Journal of Information Security and Applications*, vol. 37, pp. 50-64, 2017.

[15] G. Zhang, W. Gong, "The research of access control based on UCON in the in- ternet of things," *Journal of Software*, vol. 6, no. 4, 2011.

[16] Anggorojati, B. , Mahalle, P.N., Prasad, N.R., "Secure Access Control and Authority Delegation Based on Capability and Context Awareness for federated IoT," in *Internet of Things and M2M Communications*, River Publisher, 2013, pp. 135-160.

[17] P. Mahalle, "Identity authentication and capability based access con- trol (IACAC) for the internet of things," *Journal of Cyber Security and Mobility*, vol. 1, pp. 309-348, 2013.

[18] L. Gong, "A secure identity-based capability system," in *IEEE Symposium on Security and Privacy*, 1989.

[19] Sergio Gusmeroli, Salvatore Piccione, Domenico Rotondi, "A capability-based security approach to manage access control in the Internet of Things," *Mathematical and Computer Modelling*, vol. 58, pp. 1189-1205, 2013.

[20] Lo -Yao Yeh, Pei-Yu Chiang, Yi-Lang Tsai and Jiunand Jiun-Long Huang, "Cloud-based Fine-grained Health Information Access Control Framework for Lightweight IoT Devices with Dynamic Auditing and Attribute Revocation," *IEEE Transactions on Cloud Computing*, vol. PP, no. 99, 2015.

[21] Fagen Li , Yanan Han , Chunhua Jin, "Practical access control for sensor networks in the context of the Internet of Things," *Elsevier Computer Communications*, Vols. 89-90, pp. 154-164, 2016.

[22] Sudha Patel, Dhiren R. Patel, Ankit P. Navik, "Energy Efficient Integrated Authentication and Access Control Mechanisms for Internet of Things," in *IEEE International Conference on Internet of Things and Applications (IOTA)*, 2016.

[23] Aafaf Ouaddah ; Imane Bouij-Pasquier ; Anas Abou Elkalam ; Abdellah Ait Ouahman, "Security analysis and proposal of new access control model in the Internet of Thing," in *IEEE International Conference on Electrical and Information Technologies (ICEIT)*, 2015.

[24] Savio Sciancalepore, Giuseppe Piro, Daniele Caldarola, Gennaro Boggia and Giuseppe Bianchi, "OAuth-IoT: an access control framework for the Internet of Things based on open standards," in *IEEE Symposium on Computers and Communications (ISCC)*, 2017.

[25] Md. Eshrat E. Alahi, Najid Pereira-Ishak, Subhas Chandra Mukhopadhyay, Lucy Burkitt, "An Internet-of-Things Enabled Smart Sensing System for Nitrate Monitoring," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4409-4417, 2018.

[26] Noushin Poursafar, Md Eshrat E Alahi, and Subhas Mukhopadhyay, "Long-range Wireless Technologies for IoT Applications: A Review," in *IEEE Eleventh International Conference on Sensing Technology (ICST)*, 2017.

[27] An Braeken, Madhusanka Liyanage, Anca Delia Jurcut, "Anonymous Lightweight Proxy Based Key Agreement for IoT," *Springer Wireless Personal Communications*, p. 345–364, 2019.

[28] Anca Jurcut, Tom Coffey and Reiner Dojen, "A Novel Security Protocol Attack Detection Logic with Unique Fault Discovery Capability for Freshness Attacks and Interleaving Session Attacks," *IEEE Transactions on Dependable and Secure Computing*, 2017.

[29] Abdallah Zoubir Ourad, Boutheyna Belgacem, and Khaled Salah, "Using Blockchain for IOT Access Control and Authentication Management," in *Third International Conference Held as Part of the Services Conference Federation, SCF 2018*, 2018.

[30] S. Savinov, "A Dynamic Risk-Based Access Control Approach: Model and Implementation," *PhD Thesis, University of Waterloo*, 2017.

[31] F. Salim, "Approaches to Access Control Under Uncertainty," *PhD Thesis, Queensland University of Technology*, 2012.

[32] A. Ferreira, R. Cruz-Correia and L. Antunes, "How to Break Access Control in a Controlled Manner," in *19th IEEE International Symposium on Computer-Based Medical Systems*, 2006.

[33] Schefer-Wenzl, S., & Strembeck, M., "Generic Support for RBAC Break-Glass Policies in Process-Aware Information Systems," in *28Th Annual ACM Symposium on Applied Computing*, 2013.

[34] Molloy, I., Dickens, L., Morisset, C., Cheng, P. C., Lobo, J., & Russo, A., "Risk-Based Security Decisions under Uncertainty," in *Proceedings of the Second ACM Conference on Data and Application Security and Privacy*, 2012.

[35] Alireza Shameli-Sendi, Rouzbeh Aghababaei-Barzegar, Mohamed Cheriet, "Taxonomy of information security risk assessment (ISRA)," *computers & security* , vol. 57, pp. 14-30, 2016.

[36] Khalid Zaman Bijon, Ram Krishnan, Ravi Sandhu, "A framework for risk-aware role based access control," in *IEEE Conference on Communications and Network Security (CNS)*, 2013.

[37] Hany F. Atlam1, 2, Ahmed Alenezi1, Robert J. Walters1, Gary B. Wills1, Joshua Daniel, "Developing an adaptive Risk-based access control model for the Internet of Things," in *IEEE International Conference on Internet of Things (iThings)*, 2017.

[38] Hemanth Khambhammettu, Sofiene Boulares, Kamel Adi, Luigi Logrippo, "A framework for risk assessment in access control systems," *Elsevier Computers and Security*, vol. 39, pp. 86-103, 2013.

[39] Jason R.C. Nurse, Sadie Creese, David De Roure, "Security Risk Assessment in Internet of Things Systems," *IT Professional* , vol. 19, no. 5, pp. 20-26, 2017.

[40] Giuseppe Petracca, Frank Capobianco, Christian Skalka, Trent Jaeger, "On Risk in Access Control Enforcement," in *Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies*, Indianapolis, Indiana, USA, 2017.

[41] Zhao, Z., Hu, H., Ahn, G. J., & Wu, R., "Risk-aware mitigation for MANET routing attacks.," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 250-260, 2012.

[42] H. Reza Ghorbani ; M. Hossein Ahmadzadegan, "Security challenges in internet of things: survey," in *IEEE Conference on Wireless Sensors (ICWiSe)*, 2017.

[43] Mario FRUSTACI ; Pasquale PACE ; Gianluca ALOI ; Giancarlo FORTINO, "Evaluating critical security issues of the IoT world: Present and Future challenges," *IEEE Internet of Things Journal* , pp. 2327-4662, 2017.

[44] "What is fuzzy modeling?," in *Insight into Fuzzy Modeling*, Wiley, 2016.

[45] Y. Sakai, "J. M. Keynes on probability versus F. H. Knight on uncertainty: reflections on the miracle year of 1921," *Springer Japan Association for Evolutionary Economics*, 2016.

[46] ZHIGUO ZENG, RUI KANG, MEILIN WEN and AND ENRICO ZIO, "A Model-Based Reliability Metric Considering Aleatory and Epistemic Uncertainty," *IEEE Access Journal*, vol. 5, 2017.

[47] G. Shafer, A mathematical theory of evidence, Princeton University, 1976.

[48] Baudrit, C. and Dubois, D., "Practical representations of incomplete probabilistic knowledge," *Elsevier Journal of Computational Statistics & Data Analysis*, vol. 51, no. 1, 2006.

[49] L. B, Uncertainty Theory, Springer, 2017.

[50] Nick Firoozye, Fauzian Arrif, Managing Uncertainty Mitigation Risk, Springer, 2016.

[51] J. Bancroft, Tolerance of Uncertainty, Author House, 2014.

[52] "Towards Fuzzy Type Theory with Partial Functions," *Springer Journal of Advances in Fuzzy Logic and Technology* , 2018.

[53] K.Z. Bijon, R. Krishnan, R.S. Sandhu, "Risk-aware RBAC sessions," in *IEEE 8Th International Conference on Information Systems Security, (ICISS)*, 2012.

[54] N. Baracaldo, J. Joshi, "A trust-and-risk aware RBAC framework: tackling insider threat," in *ACM Proceedings of the 17th Symposium on Access Control*, 2012.

[55] N. Baracaldo, J. Joshi, "An adaptive risk management and access control framework to mitigate insider threats," *Elsevier Journal of Computers & Security*, vol. 39, pp. 237-254, 2013.

[56] N. Dimmock, A. Belokosztolszki, D. Eyers, J. Bacon, K. Moody, "Using trust and risk in role-based access control policies," in *ACM Symposium on Access Control Models and Technologies (SACMAT)*, 2014.

[57] L. Chen, J. Crampton, "Risk-aware role-based access control," in *International Workshop on Security and Trust Management, Cited by Springer*, 2012.

[58] D.R. dos Santos, C.M. Westphall, C.B. Westphall, "Risk-based dynamic access control for a highly scalable cloud federation," in *IEEE Proceedings of the Seventh International Conference on Emerging Security Information, Systems and Technologies*, 2013.

[59] D.R. dos Santos, C.M. Westphall, C.B. Westphall, "A dynamic risk-based access control architecture for cloud computing," in *IEEE Network Operations and Management Symposium (NOMS)*, 2014.

[60] Daniel Ricardo dos Santos, Roberto Marinho,Gustavo Roecker Schmitt, "A framework and risk assessment approaches for risk-based access control in the cloud," *Elsevier Journal of Network and Computer Applications*, vol. 74, 2016.

[61] Hany F. Atlam, Ahmed Alenezi, Robert J. Walters, Gary B. Wills, Joshua Daniel, "Developing an adaptive Risk-based access control model for the Internet of Things," in *IEEE International Conference on Internet of Things*, 2017.

[62] Sadegh Dorri Nogoorani, Rasool Jalili, "TIRIAC: A trust-driven risk-aware access control framework for Grid environments," *Future Generation Computer Systems*, vol. 55, pp. 238-254, 2016.