Context-Driven IoT Management: A Step Closer Towards A Self-Governing IoT

Bel G. Raggad
Seidenberg School
Pace University, New York, USA

Abstract

Despite the adequate computing power available at the edge, fog, and cloud layers, IoT management is still performed very hastily. IoT actuators may make the hosting devices autonomous but not the IoT. IoT which are meant to be self-governing are still far from getting there. This paper, by proposing a context-driven IoT management process, brings us a step closer to a self-governing IoT. IoT contexts are envelopes of data from various IoT devices that can be evaluated by devices or humans to recognize one or more events that call for actions that are performed by humans or which are automatically evoked. An IoT comprises operational contexts at the edge, functional contexts at the fog, and strategic contexts at the cloud. IoT contexts, whether they are written in terms of auditable deterministic scripts, or belief structures, are however always tainted with a great deal of uncertainty that, due to the presence of ambiguities and inconsistencies, cannot be managed in a Bayesian manner. We hence apply Dempster and Shafer theory to perform context-driven IoT management. In order to do so, IoT contexts are written into polynomial contexts in a hierarchic manner from cloud to edge. Context-driven IoT management is modeled as polynomials of strategic contexts that are written as polynomials of functional contexts which are in their turn written as polynomials of operational contexts for which belief structure are constructed based on edge data. This paper provides a simple and detailed example to demonstrate the working of our context-driven IoT management model.

Keywords: IoT, context, edge computing, fog computing, cloud computing, Dempster and Shafer Theory

1. Introduction

The idea of connecting objects together and granting them some degree of computing power and intelligence have been around many years before Kevin Ashton introduced the internet of things (IoT) in 1999 [1][2]. Due to the limitation in needed technology this new concepts started very slowly on many years. For a faster growth, IoTs needed advances in communication to allow for cellular, satellite, and LAN connectivity solutions and specific protocols for sharing data among [3]. Additionally, they needed a technology that allows them to gather, manage, process, and analyze the data generated by devices that can sense events and contexts and act accordingly [4]. The IoT technology has enabled organizations to enhance their efficiency by automating their production and logistics [5][6]. IoT permitted a transparent and visible supply chain that allowed companies to reduce inventory costs and improve service delivery. While IoT is in great use in manufacturing, transportation, and utility organizations [7], we started seeing IoT almost everywhere, including healthcare, agriculture, and automotive. Companies needed to rethink their business processes and production systems and reconfigure them to more closely monitor and control these processes in order to provide a better business decision support that will reduce production costs, improving customer service, enhancing productivity, and increasing revenues. This decision supports capability that IoT brought can produce useful insights that touch all business activities from production and supply chain to quality assurance, logistics, and customer loyalty [8].

In the absence of a universal definition of IoT, this paper defines an IoT as an open network of smart internet-enabled devices capable of recognizing contexts that call for actions and capable of sharing data, information, and resources.

2. IoT management model description

In the absence of a universal definition of IoT, this paper defines an IoT as an open network of smart internet- enabled devices capable of recognizing contexts that call for actions and capable of sharing data, information, and resources.

The IoT may be managed just by defining contexts that can be recognized by either devices themselves or by owners. These contexts are called predefined contexts because they were defined at the beginning of the IoT cycle to track the behaviors of the IoT,

 | DOI: 10.20533/ijicr.2042.4655.2024.0149

technically, economically, operationally, socially, and legally/ethically. Owners, however, can at any time define new contexts to audit for some claimed assertions, to inspect or verify some specific situations, or to add some supplementary managerial interventions. These contexts are called interventional contexts. All contexts are represented by events described by one or more random parameters associated with various types of uncertainties including a great deal of ambiguities and inconsistencies. This type of uncertainty will make it unsuitable to Bayesian reasoning. All predefined and interventional contexts adopted in IoT management are modeled as belief structures that are studied using Dempster and Shafer Theory.

IoT management activities may be written as contexts with unknown belief structures. Operational data are used to construct belief structures on the operational contexts, as shown in Figure 1. These beliefs are then propagated for the predefined functional contexts. These functional contexts are now having belief structures that we will propagate to the strategic contexts. At this point, we have belief structures for all the predefined structures associated with operational, functional, and strategic contexts. We can now fuse these belief structures conjunctively and obtain an idea on IoT management.

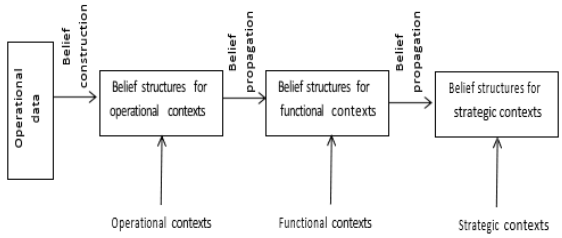


Figure 1. Belief construction and propagation

Our model consists of 4 phases: Context-based edge management, Context-based fog management, Context- based cloud management, and Overall context-based IoT management. The phases are made of following computational steps:

Phase 1: Context-based edge management

Step 1.1: Edge processing for predefined operational contexts

Step 1.2: Edge managerial actions

Step 1.3: Edge processing for interventional operational contexts

Phase 2: Context-based fog management

Step 2.1: Fog processing for predefined functional contexts

Step 2.2: Fog managerial actions

Step 2.3: Fog processing for interventional functional contexts

Phase 3: Context-based cloud management

Step 3.1: Cloud processing for predefined strategic contexts

Step 3.2: Cloud managerial actions

Step 3.3: Cloud processing for interventional strategic contexts

Phase 4: Overall context-based IoT management

Step 4.1: Overall context-based IoT evaluation

Step 4.2: IoT managerial actions

3. Definition of IoT contexts

Without any loss of generalities, we assume that contexts are mainly events represented by one parameter. This parameter is often uncertain with unknown belief structure. These contexts may be written as polynomials made of contexts at the same level and contexts one level underneath, as depicted in the context hierarchy in Figure 2. That is, a dependent context is written in terms of many independent contexts, as products and sums. All independent terms in the polynomial are with belief structures that can be propagated to the dependent context. The contexts at the hierarchy leaves add operational contexts that have known belief structures by construction. We use operational data on the relevant parameters to construct belief structures on the operational contexts.

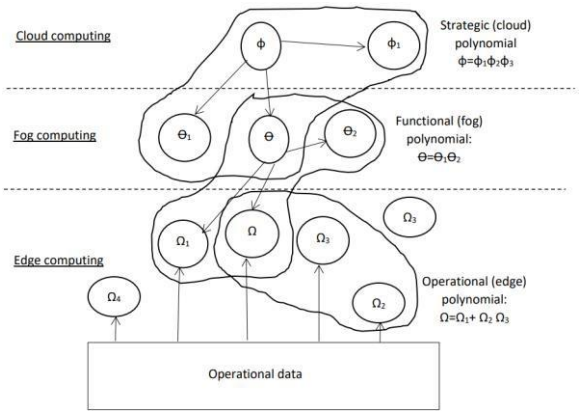


Figure 2. Context hierarchy

IoT contexts consist of data from different IoT data sources that can be evaluated by devices or humans to recognize one or more events that call for actions that are performed by humans or which are automatically evoked. An IoT comprises operational contexts at the edge, functional contexts at the fog,

 | DOI: 10.20533/ijicr.2042.4655.2024.0149

and strategic contexts at the cloud. Even though IoT contexts, whether they are operational, functional, or strategic, and whether they are written in terms of auditable deterministic scripts, or belief structures, they are always tainted with a great deal of uncertainty that cannot be managed in a Bayesian manner due to the ambiguities and inconsistencies in it. Hence Dempster and Shafer theory was applied to realize context-based IoT management. In order to do so, IoT contexts are written as polynomial contexts in a hierarchic manner. Context- based IoT management is modeled as polynomials of strategic contexts which are written as polynomials of functional contexts which are in their turn written as polynomials of operational contexts that are evaluated using edge data.

Computational support to produce belief structures is obtained by constructing evidential mapping matrices elicited from IoT owners. Frames of discernment at a lower level is propagated to the next higher level using the evidential mapping matrices, from the operational level to the functional level, and from the functional level to the strategic level. Without loss of generalities, we assume that all operational contexts share the same frame of discernment $\Omega = \{\varphi_1, \ldots, \varphi_N\}$, and all functional contexts share the same frame of discernment $\Theta = \{\Theta_1, \ldots, \Theta_M\}$, and all strategic contexts share the same frame of discernment $\phi = \{\phi_1, \ldots, \phi_K\}$. This assumption is needed to ease the computations involved in our proposed model. For example, we can assume that all frames of discernment of operational contexts are similar and fixed as Ω = {u, n, f} = {u='At a state unfavorable to IoT management objectives', n='At a state neutral to IoT management objectives', f='At a state favorable to IoT management objectives'}. Of course, any data generated by a target device can always be transformed into the states {u, n, f}. We can do the same for functional and strategic contexts. Context-based IoT management is like writing a long and hierarchic behavioral script describing in details the acceptable behavior of the IoT. A context will be a verifiable small script unit represented by a parameter for which we either know the belief structure or which is related to another parameter, using an evidential mapping matrix, for which we know the belief structure. Belief propagation will be applied in this case to construct a belief structure for the parameter without one, as long as there is heuristic knowledge that defines the evidential link needed for the belief propagation process. Strategic contexts will be scripts defining the verifiable behavior of the IoT for a long-term period, say about 2 to 3 years. The functional contexts will be scripts defining the verifiable behavior of the IoT for a midterm period, say about 6 months to a year. The operational contexts will be scripts defining the verifiable behavior of the IoT in day-to-day IoT operations and for short term periods, say about days and weeks. Figure 3 depicts an example of the layout of strategic contexts written as polynomials of functional and strategic contexts.

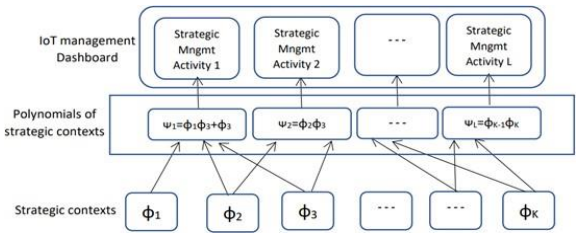


Figure 3. An example of a layout for strategic contexts

4. Belief Structure Construction for Operational Constructs in the Edge Layer

In order to combine the contexts, we need to redefine them on the same frame of discernment. This is done by considering each focal element and find the best subset in {u, n, f} equivalent to it. If two or more mass values are produced for the same focal element, the average mass value is assigned to the new focal element. This way, we will go from a belief function built on its frame of discernment to a belief function built on {u, n, f}. We will need to transform the overall operational, overall functional, and overall strategic contexts to be redefined on the same frame of discernment {u, n, f}. Once we are done with this, we can simply combine them using Dempster Rule of Combination. The same transformation may be applied of the interventional context if an overall audit evaluation is needed on specific situations of the working of the IoT. Figure 4 depicts the construction of a belief structure for IoT operational data.

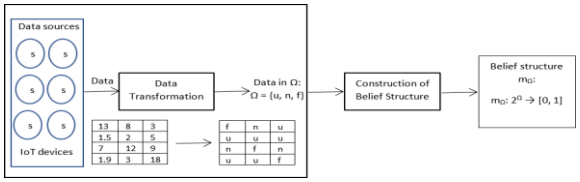


Figure 4. Construction of a belief structure for IoT operational data

For example, if a context has its belief structure as follows:

$\Omega = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$m: 2^{\Omega} \rightarrow [0, 1]$

where:

$m(\{5, 9, 10\}) = .3$

$m(\{2, 3\}) = .1$

$m(\Omega) = .6$

This belief structure may be transformed into the following:

$\Omega = \{u, n, f\}$

$m: 2^{\Omega} \rightarrow [0, 1]$

where:
$m(\{n, h\}) = .3$
$m(\{u\}) = .1$
$m(\Omega) = .6$

In certain cases, we may produce two mass values for one focal element like when we have $m(\{5, 9, 10\}) = .3$ and $m(\{6, 8\}) = .1$. These focal elements will produce $m(\{n, h\}) = .3$ and $m(\{n, h\}) = .1$. In this case, we use the average as mass value and obtain $m(\{n, h\}) = .2$.

After the operational data generated by the data sources is transformed into Ω range, we can start the construction of its belief structure with Ω as the frame of discernment.

Consider data source data as $D=\{D_1, \ldots, D_N\}$ and $E=\{E_1, \ldots, E_N\}$ where $E_i = 2D_i$, and let e be a hypertuple of E. Also let Δ be a partial order relation on all the data sets on hand. If x and y are elements of a set E, we say that $x \Delta y$ if and only if $x \subseteq y$. The inclusion defines the amount of support x provides to y, or alternatively, the amount of compatibility between x and y. We define the evidence support $S_D(x)$ of x in D as the set of y in D such that $y \Delta x$. That is, $S_D(x) = \{y \varepsilon D$, such that $y \Delta x\}$. The subset D is a posit with respect to the partial order relation Δ and it may hence have elements that are related to x (fully compatible) and others that are not related to x (not fully compatible). Only the compatible elements y in D such that $y \Delta x$ are accepted to support x.

$m_D: 2^E \rightarrow [0\ 1]$

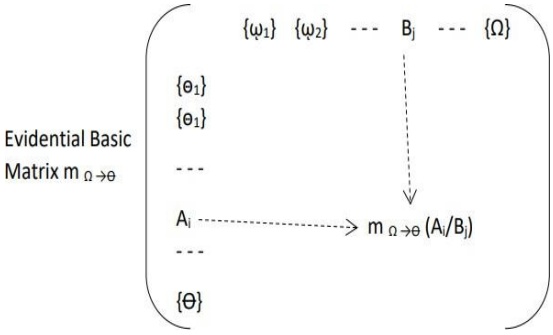
$m_D(x) = |S_D(x)| / |S_D(E)|$

where $S_D(E) = \{y \varepsilon D$ such that $y \Delta x\}, x \varepsilon E\}$

5. Evidential Mapping for belief propagation from Operational to Functional Constructs

At the edge layer, the only data sources we have are sensors embedded in devices used to control and monitor the domain environment for which the IoT is configured. At the planning phase of the IoT projects, owners define the purposes of all devices and their sensors and more importantly any contexts at the operational, functional, or strategic levels that they needed to secure the business continuity of the IoT system. Owners should be fully informed of all IoT contexts at all levels and also well informed of all possible evidential links between operational contexts and functional contexts and between functional contexts and strategic contexts. The elicited evidential mapping matrices that are produced through heuristic knowledge will serve in the propagation of beliefs from one level to a higher level and in the computational of belief structures at all levels.

Let $\Omega = \{\wp_1, \ldots, \wp_N\}$ be an operational context for which we know a belief structure and let $\Theta = \{\Theta_1, \ldots, \Theta_M\}$ a functional context for which we don't know the belief structure but for which we will construct a belief structure using belief propagation. The evidential basic matrix gives evidential mapping between subsets A_i of Ω, on the colons of the matrix and subsets B_j of Θ on the rows of the matrix as follows:



The result of propagating the belief on the operational context Θ to the functional context Ω is given by basic belief assignment $m\ \Omega \rightarrow \Theta$ as follows:

$m_{\Omega \rightarrow \Theta}: 2^{\Theta} \rightarrow [0, 1]$

$m_{\Omega \rightarrow \Theta}(X) = \sum_{Y \leq 2^{\Omega}} m(Y)\ m_{\Omega \rightarrow \Theta}(X/Y)$

6. IoT Context-Driven Management Process

IoT management is a continuous process even though more intense and more frequent at the operational level as part of edge computing where all the data is produced. This data will be transmitted to the cloud where it resides awaiting its delayed process. Some of this data may be stored temporarily for a very short period to see if some urgent actions may be taken to update IoT devices, reconfigure, or correct their operations. As part of IoT operational management, predefined contexts are present to monitor and evaluate device operations. In addition to the predefined contexts, operational management may write some interventional operational contexts and process them to evaluate certain operational aspects of the audited devices. In a similar way, there will be predefined functional contexts needed to control the working of the devices, and also some interventional functional contexts as needed for working aspects of the IoT. There will also be predefined strategic contexts to implement some long- term objectives of the IoT and some interventional strategic context

 | DOI: 10.20533/ijicr.2042.4655.2024.0149

when new objectives or goals are evaluated. This IoT context-based management process is depicted in Figure 5.

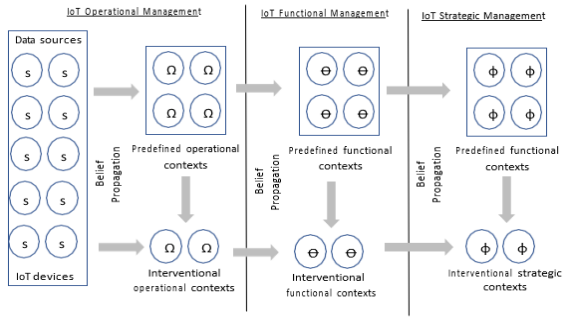


Figure 5. Layout for context-based IoT management

7. Context polynomial belief propagation

A polynomial context φ is the sum of products of contexts for which we know their belief structures. This equation made of contexts contains sums of contexts and products of contexts. While use Dempster Rule for combining evidence for both the sums and the products, this rule is applied for the products in a conjunctive manner and for the sums in a disjunctive manner.

Suppose we have two belief functions with their basic belief assignments m_1 and m_2 on **Ω**, when m1 and m_2 are combined the product $m_1(A)m_2(B)$, $A,B \leq \Omega$ is allocated to AΛB in the Conjunctive Dempster Rule (CDR) of combination as follows:

For any X in **Ω**, $m_1(\Lambda)m_2(X) =$

$$\sum_{x= A \Lambda B} m_1(A)m_2(B)$$

On the other hand when m_1 and m_2 are combined the product $m_1(A)m_2(B)$, $A,B \leq \Omega$, is allocated to AVB in the Disjunctive Dempster Rule (DDR) of combination as follows:

For any Y in **Ω**, $m_1(\Lambda)m_2(Y) =$

$$\sum_{Y= AVB} m_1(A)m_2(B)$$

That is, if we have $\Theta = \Omega_1\Omega_2 + \Omega_3$, then we will use the conjunctive Dempster Rule to combine Ω_1 and Ω_2 and use the Disjunctive Dempster Rule to combine the product $\Omega_1\Omega_2$ and Ω_3. Figure 6 depicts the belief propagation process.

Predefined contexts at the operational, functional, or strategic levels can be combined to produce an evaluation of the working of the IoT. These contexts will predict any behavioral aspects that IoT management expect to see throughout the life cycle of the IoT. The belief structures on the predefined contexts may also be used to produce Pignistic probabilities of important states of the IoT that can be used to estimate operational, functional, or strategic risks. Combining the predefined contexts will give an actionable evaluation of the working of the IoT. Interventional contexts are usually evoked to check or verify some specific situations at the operational, functional, or strategic levels of IoT management.

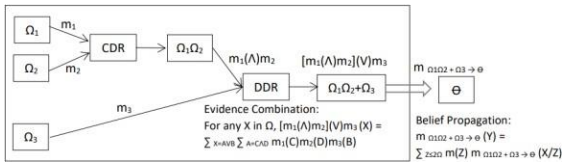


Figure 6. Belief propagation process

Combining the interventional contexts will produce an evaluation of specific situations that need to be audited. Figure 7 depicts how edge, fog, and cloud computing relate to contextual processing.

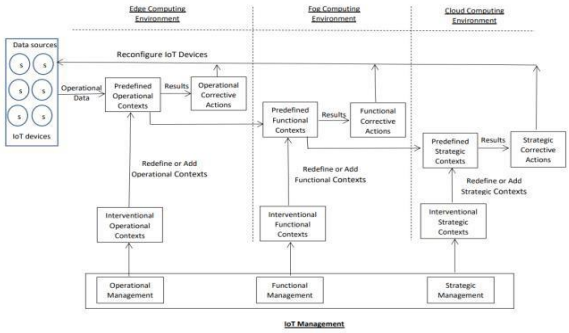


Figure 7. Belief Propagation Process

8. Simple Example of an Inventory IoT

In this example, an IoT is charged of inventory management. Contexts at all managerial levels are defined using simple parameters. We show how to create belief structures for operational data at the edge level and how to propagate these beliefs to functional contexts at the fog level. The obtained belief structures at the fog level are propagated to strategic contexts at the cloud level. Remember all data in an IoT originates at the devices where operational data is created. While some of this data will be extracted and stored at the edge or at the fog for needed processes, all the data will permanently (throughout its lifecycle) reside in the cloud. Figure 8 depicts the layout of the contexts written to manage the inventory IoT.

A simple example, in Figure 9, to demonstrate how does the belief construction works. Assume a group of IoT devices generates data that is store temporarily in edge computing in a data set D. As you can see the data in D belongs to a domain different from the frame of discernment **Ω** defined for operational contexts. The data set D has to be

 | DOI: 10.20533/ijicr.2042.4655.2024.0149

transformed into the range of **Ω** as shown below. We can now construct the belief structure on **Ω**. The subsets of **Ω** with positive masses are the focal elements of the basic belief assignment built on **Ω**. As you can see, the focal elements are {m}, {h}, {l, m}, {l, h}, {m, h} and {l, m, h}.

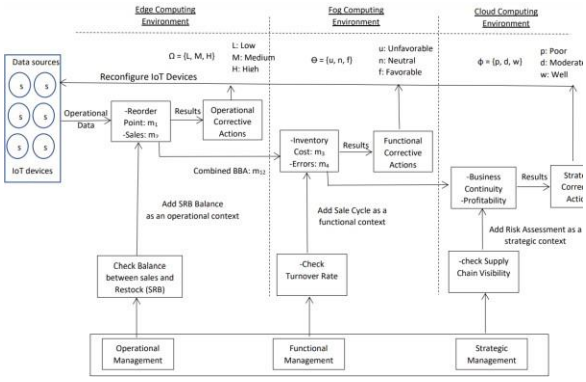


Figure 8. Layout of the contexts written to manage the inventory IoT

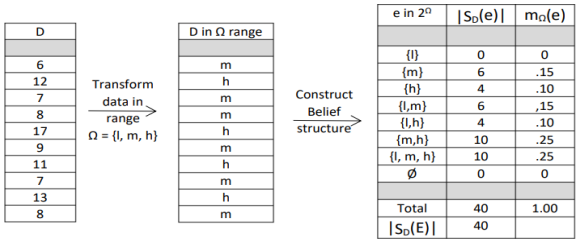


Figure 9. A simple example of constructing a belief structure from operational data with a single attribute

Once we constructed the belief structure on the operational context **Ω**, we now need to obtain from owners, the evidential mapping matrix that defines the evidential link between the operational structure **Ω** and the functional context **Θ**. Thins link defines the evidential mapping between the subsets of **Ω** and the subsets of **Θ** (see Table 1).

Table 1. Evidential Mapping Between Operational and Functional Contexts

Evidential mapping between the subsets of Ω and the subsets of Θ								
	{l}	{m}	{h}	{l, m}	{l, h}	{m, h}	{l, m, h}	{Ø}
{u}	.0	.1	.4	0	0	0	0	0
{n}	.2	.4	.2	0	0	0	0	0

$$m_{\Omega\to\Theta} = \begin{pmatrix} .0 & 0.1 & 0.4 & .0 & .0 & .0 & .0 \\ 0.2 & 0.4 & 0.2 & .0 & .0 & .0 & .0 \\ 0.4 & 0.1 & .0 & .0 & .0 & .0 & .0 \\ .0 & .0 & .0 & .0 & .0 & .0 & .0 \\ .0 & .0 & .0 & .0 & .0 & .0 & .0 \\ .0 & .0 & .0 & .0 & .0 & .0 & .0 \\ 0.4 & 0.4 & 0.4 & 1 & 1 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} .0 \\ 0.15 \\ 0.1 \\ 0.15 \\ 0.1 \\ 0.25 \\ 0.25 \end{pmatrix} = \begin{pmatrix} 0.055 \\ 0.08 \\ 0.015 \\ .0 \\ .0 \\ .0 \\ 0.85 \end{pmatrix}$$

As shown in Table 1, the selected functional context has a belief structure that we obtained by propagating the belief constructed on the backorder rate date obtained from operational data generated by edge data sources. The evidential matrix between functional and strategic contexts is given in Table 2. The functional context is hence defined as follows:

$m_{\Omega\to\Theta} : 2^{\Theta} \to [0\ 1]$
where:
$m_{\Omega\to\Theta}(\{u\}) = .055$
$m_{\Omega\to\Theta}(\{n\}) = .08$
$m_{\Omega\to\Theta}(\{f\}) = .015$
$m_{\Omega\to\Theta}(\{\Theta\}) = .85$

Table 2. Evidential Mapping Between Functional and Strategic Contexts

Evidential mapping between the subsets of Θ and the subsets of ϕ								
	{u}	{n}	{f}	{u, n}	{u, f}	{n, f}	{u, n, f}	{Ø}
{p}	.4	0	0	0	0	0	.2	.0
{d}	.1	.4	.1	0	0	0	.1	.0
{w}	0	0	.4	0	0	0	0	.0
{p, d}	0	0	0	0	0	0	0.2	.0
{p, w}	0	0	0	0	0	0	.1	.0
{d, w}	0	0	0	0	0	0	0	.0
{p, d, w	.5	.6	..5	1	1	1	.4	.0
{Ø}	0	0	0	0	0	0	0	.0

$$\begin{pmatrix} .4 & .0 & .0 & .0 & .0 & .0 & .2 & .0 \\ .1 & .4 & .1 & .0 & .0 & .0 & .1 & .0 \\ .0 & .0 & .4 & .0 & .0 & .0 & .0 & .0 \\ .0 & .0 & .0 & .0 & .0 & .0 & .2 & .0 \\ .0 & .0 & .0 & .0 & .0 & .0 & .1 & .0 \\ .0 & .0 & .0 & .0 & .0 & .0 & .0 & .0 \\ .5 & .6 & ..5 & 1 & 1 & 1 & .4 & .0 \\ .0 & .0 & .0 & .0 & .0 & .0 & .0 & .0 \end{pmatrix} \times \begin{pmatrix} .055 \\ .08 \\ .015 \\ .0 \\ .0 \\ .0 \\ .85 \\ .0 \end{pmatrix} = \begin{pmatrix} .192 \\ .006 \\ .085 \\ .124 \\ .17 \\ .0 \\ .423 \\ .0 \end{pmatrix}$$

The strategic context is hence defined as follows:

$m_{\Theta\to\phi} : 2^{\phi} \to [0\ 1]$
where:
$m_{\Theta\to\phi}(\{p\}) = .192$
$m_{\Theta\to\phi}(\{d\}) = .006$
$m_{\Theta\to\phi}(\{w\}) = .085$
$m_{\Theta\to\phi}(\{p, d\}) = .124$
$m_{\Theta\to\phi}(\{p, w\}) = .17$
$m_{\Theta\to\phi}(\{\phi\}) = .423$

9. Managerial implications

Management actions whether they are at the operational, functional, or strategic level, are based on decisional information and insights that often value or verify some relevant assertions. The assertions are often binary variable taking True or False values, or categorical variables taking values on some Likert scales.

It is important to note that in an IoT, the only data we have, stored at the edge layer, or stored at the fog or cloud layers, is data that is originally obtained from IoT devices underneath the operational level.

Contexts and other IoT parameters at the edge, fog, or cloud layer, do not really have their own proper data, but they process data or information, that originated at the IoT devices. That is, every managerial action is therefore associated with a context or composite context that can be written in

 | DOI: 10.20533/ijicr.2042.4655.2024.0149

terms of contexts at the same managerial level or at a level underneath. For example, a strategic context is written in terms of other strategic contexts and functional contexts in a polynomial form. The same way, a functional context is written in terms of other functional contexts and operational contexts. This obviously implies that all management activities can be written in contexts that can be configured as part of the IoT configuration. This will certainly give some self-governing capability to the IoT. While the IoT is running on its own, IoT management can always intervene using interventional contexts that are written in the same way as the predefined contexts that are configured with the configuration of the IoT.

In addition to interventional contexts, IoT management can always be interested in evaluating some comprehensive tendencies in IoT operations or in assessing some overall risk aspects associated with the IoT feasibility of its business continuity. In most of those cases, those evaluations can be written in terms of contexts as in interventional contexts.

10. Conclusion

In order to advance towards a self-governing IoT system, the article proposed a context-based IoT management process. IoT contexts were defined as envelopes of data generated by various IoT devices that are often associated with one specific assertion or a set of related assertions defining some trends in IoT operations. These contexts can be evaluated by devices or humans to recognize one or more events that call for actions that are performed by humans or which are automatically evoked. Our model dealt with operational contexts at the edge layer, functional contexts at the fog layer, and strategic contexts at the cloud layer. These contexts are tainted with a great deal of uncertainty. Due to the presence of ambiguities and inconsistencies in IoT uncertainty, Bayesian reasoning cannot be applied. We hence modeled contexts as belief structures and applied Dempster and Shafer Theory to process them. IoT contexts are written into polynomial contexts in a hierarchic manner from cloud to edge. Context-driven IoT management was modeled as polynomials of strategic contexts that are written as polynomials of functional contexts. These functional contexts are in their turn written as polynomials of operational contexts for which belief structures are constructed based on edge data. The paper provided a detailed example to demonstrate the working of our context-driven IoT management model.

11. References

[1] Hoffmann, J. B. Heimes, P. and Senel, S. 2019). IoT Platforms for the Internet of Production, in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4098-4105, June.

[2] Kumar, S. et al. (2019). Internet of Things is a revolutionary approach for future technology enhancement: A review. J Big Data 6, 111.

[3] D. Minoli, et al., (2017). IoT security (IoTSec) considerations, requirements, and architectures. In the Proceeding of 14th IEEE annual consumer communications and networking conference (CCNC), Las Vegas, NV, USA, 8–11 January. DOI: 10.1109/ccnc.2017.7983 271.

[4] Muhammad, I.T., and Noviyanti, W.S. (2023). Artificial Intelligence of Internet of Things (AIoT) Technology-based Law Enforcement Process. IOTA. ISSN 2774-4353, Vol.03, 01.

[5] Koohang, A. et al., (2022). Internet of Things (IoT): From awareness to continued use, International Journal of Information Management, Volume 62.

[6] Mehta, R. et al., (2018). Internet of Things: Vision, Applications and Challenges, Procedia Computer Science, Volume 132, Pages 1263-1269.

[7] Gaona-Garcia, et al., (2017). Analysis of security mechanisms P. based on clusters IoT environments. Int J Interactive Multimedia Artificial Intelligence. 4(3):55–60.

[8] Saravanan, G. et al., (2022). Implementation of IoT in production and manufacturing: An Industry 4.0 approach, Materials Today: Proceedings, Volume 51, Part 8.

 | DOI: 10.20533/ijicr.2042.4655.2024.0149