DOI: https://doi.org/10.24297/ijmit.v14i0.7919

Information Riskswith Internet of Things inCultural Creative Industry

Der-Ren Hsu

Department of Tourism and Leisure Management, Tung-Fang Design University, Kaohsiung, Taiwan, ROC.

hsudren@gmail.com

Abstract

Internet of Things (IoT) is characterized by various technologies, which are in accord tothe provisioning of innovative services in innumerable application domains. In cultural creative industry, Internet of things has been widelypracticed now, and will still have many creative potential in art work applications. In this consequence,the satisfaction of risk management requirements plays a fundamental role.Unfortunately, there is little objective, scientific research focused on evaluating the risksof security issues that result from information exchange among Internet of Things. In this study, the Grey Relational Analysis (GRA) is employed to identify and evaluate the risks of IoT. This research finds that Privacy, Access Control, and Trust are the top three risk factors.UsingIoT in cultural creative industry is a new inevitable business trend, it is an unavoidableresponsibility to our society to govern and constitute a healthy environment for all the related users.

Indexing terms/Keywords:Information management, Internet of Things, Cultural creative, GRA.

Subject Classification: Information management, Cultural creative industry

Type (Method/Approach): Survey/Interview

Introduction

The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, and connectivity which enable these objects to connect and exchange data, and interoperate as a team machines in the internet infrastructure. Experts estimate that the IoT will consist of about 30 billion objects by 2020[1]. "Things", in the IoT sense, can refer to a wide variety of devices such as automobiles with built-in sensors,biochip transponders on farm animals, cameras streaming live feeds of wild animals in coastal waters, heart monitoring sensors,DNA analysis devices for environmental/food/pathogen monitoring[2], or field operation devices that assist firefighters in search and rescue operations[3].

In 2018IoT propelled new versions of cultural creative industry, While its efforts at music composition are raising a few eyebrows, the IoT does appear to be making its way more successfully into galleries and museums, not only in the form of smart sculptures and other works of art, but also in the arena operations.Not only large scale use of IoT devices such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities for some years, but also small scale use of mobile devise in cultural creative industry as a tool for their interactive shows. Technology has progressed so rapidly that It is also estimated that the global market value of IoT will reach $7.1 trillion by 2020 [4] .

The success of the idea of connecting devices to make them more efficient is dependent upon access to and storage & processing of data. For this purpose, companies working on IoT collect data from multiple sources and store it in their cloud network for further processing. This leaves the door wide open for privacy and security dangers and single point vulnerability of multiple systems [5].

In the past ten years especially, the economy and society have changed rigorously, and not only the incomes of consumers but also the dollar amounts of purchases have risen. Consumers' habits of purchasing IoTrelated products are more different than ever. In order to occupy this market, most cultural creative industry have invested plenty of resources and man power in Iot devices in order to provide the new design opportunities and increased convenience the Internet can provide, through which customers will enjoy their IoT relatedcultural creative service.

As a result, this study has the following objectives:

1. Identify the evaluation factors attributable to IoT services using scientific and objective methods;

2. Measure and analyse the risk factors from IoT;

3. Provide administrators with the risk factors information necessary to make risk management decisions with regard to IoT;

4. Provide support for management's authorization of IoT based on objective, scientific, risk-focused assessments.

The concept of a network of smart devices was discussed as early as 1982, with a modified Coke machine at Carnegie Mellon University becoming the first Internet-connected appliance [6],able to report its inventory and whether newly loaded drinks were cold [7].In 1994 Reza Raji described the concept in IEEE Spectrum as "moving small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories"[8].

LITERATURE REVIEW

The concept of the Internet of things became popular in 1999, through the Auto-ID Center at MIT and related market-analysis publications.Radio-frequency identification (RFID) was seen by Kevin Ashton (one of the founders of the original Auto-ID Center) as a prerequisite for the Internet of things at that point [9]. Ashton prefers the phrase "Internet for things[10]." Today, the idea of IoT is widely applied that a significant transformation is to extend "things" from the data generated from devices to objects in the physical space, and it is well practiced in variabilities of any circumstances people could imagine.

In 2017, architectural designers worked with IBM supercomputer Watson to create something they've never done before. The result is The First Thinking Sculpture. It's the first sculpture that helped pick its own materials, shapes and colours [11]. The IoT does appear to be making its way more successfully into galleries and museums – not only in the form of smart sculptures and other works of art – but in the operations arena too [12]. Another well-known cultural creative IoT device, Amazon Alexa, is a voice-controlled application that is rapidly gaining popularity [13].

All those IoT applications in cultural creative industry and service are facing security issues. First,users require the "privacy" of their personal informationrelated to their movements, habits and interactions withother people. In a single term, their privacy should be guaranteed. A user-controlled privacy-preserved accesscontrol protocol is proposed, based on context-aware anonymityprivacy policies. Note that privacy protectionmechanisms are investigated: users can control which oftheir personal data is being collected and accessed, whois collecting and accessing such data, and when thishappens [14]. The traditional privacy mechanisms are dividedinto two categories: Discretionary Access and LimitedAccess. The former addresses the minimum privacy risks,in order to prevent the disclosure or the cloning of sensitivedata; whereas the latter aims at limiting the securityaccess to avoid malicious unauthorized attacks[15].

The second issue is policy "enforcement" which refers to the mechanisms used toforce the application of a set of defined actions in a system.More in details, policies are operating rules which need tobe enforced for the purpose of maintaining order, security,and consistency on data[16].As regards policy enforcement, itis suggested to use security services such as firewalls. In order toprotect the data integrity, and availability, a flexible policy enforcement framework is needed [17].

As regards "authentication", the approach presented by Zhao [18] makes use of a custom encapsulation mechanism,namely smart business security IoT application Protocol –intelligent Service Security Application Protocol.Itcombines cross-platform communications with encryption,signature, and authentication, in order to improve IoT applicationsdevelopment capabilities by establishing a securecommunication system among different things. Another idea is a two-phase authentication protocol allows the sensor nodes and the end-users to authenticate each other and initiate secure connections[19].It appears that a unique and well-defined solution ableto guarantee confidentiality in anIoT context is still constructing.

"Middleware" is another issue that is needed to be concerned. Due to the very large number of heterogeneous technologiesnormally in place within the IoT paradigm, severaltypes of middleware layer are employed to enforce theintegration and the security of devices and data withinthe same information network.Several recent works tried to address the presentedissues. Ji el. pointed out the problem of cloud-based implementation in IoT [20], and Nguel. conduct a thorough analysis of the challenges in developing an IoT middleware that holds the heterogeneity of IoT devices[21]. Also, middleware currently lacks a unified vision,able to responding to all the IoT requirements, both interms of security and privacy and network performance.

The system also incorporates certain other sensors to stop the "burglary".If an unauthorized person tries to steal the IoTvehicle, user and police station will be notified with GPS location.If the burglar tries to turn on the battery by using paperclips in the fuses then the owner will be notified about the past proceedings along with GPS location of the car. The system works well with low-price range car employed with keyless entry and self-start button and is unique because it uses IoT to protect thecars from burglary [22].

In many cases, vendor servers span multiple countries with different compliance and data privacy laws, making it unclear which legal entity has "jurisdiction" over the data [23]. One set of issues surrounds cross-border data flows, which occur when IOT devices collect data about people in one jurisdiction and transmit it to another jurisdiction with different data protection laws for processing [24]. How to manage the contract among different jurisdictions will be a universal contest in the near future.

The "trust" concept is used in various contexts and withdifferent meanings. Trust is a complex notion about whichno definitive consensus exists in the scientific literature,although its importance is widely recognized. A mainproblem with many approaches towards trust definitionis that they do not lend themselves to the establishmentof metrics and evaluation methodologies [25]. A trust management system for IoT is able to assess the trust level of a node from its past behaviourin distinct cooperative services. A trust and reputation model is recognized as animportant approach to defend a large distributed sensor networks inIoTagainst malicious node attacks, since trust establishmentmechanisms can stimulate collaboration among distributed computingand communication entities, facilitate[26].

Another problem is the "vulnerability" which is related with the storage system. In most IoT service models, enterprise data are stored externally. Because malicious users can exploit weaknesses in the data security model to gain unauthorized access to data, mobile channel vendors are urged to adopt additional security measures to prevent breaches. In other words, the use of IoT services implies system vulnerability associated with malicious employees [27].

As regards "confidentiality", it is necessary to consider various security challenges, such as a secure access provision to Internet of Things-enabled services and interoperability of security attributes between different administrative domains[28]. It is analysedhow existing key management systems could beapplied to the IoT

context.The analyses show that (a) public key cryptography can be used for sensor nodes accessing external services, (b) pre-shared key approaches can be useful for server nodes in small real-world applications, but mathematical-based KMS provide better properties if the application can afford the extra overhead[29].

"Access control" refers to the permissions in the usage ofresources, assigned to different actors of a wide IoT network.Two subjects: the data holdersand the data collectors. Users and things, as data holders,must be able to feed data collectors only with the dataregarding a specific target. At the same time, data collectorsmust be able to identify or authenticate users andthings as legitimate data holders, from which the informationare collected[19].The attention of access control is focused on the layer responsiblefor data acquisition, which is the direct responsible for theinformation collection. In such a layer, a large amount ofnodes are required to sense a wide range of different datatypes for authorized users in accordance with privacy andsecurity levels[30].

To draw a conclusion from the prior literature review (a) Privacy, (b) Enforcement, (c) Authentication, (d) Middleware, (e) Burglary, (f) Jurisdiction, (g) Trust, (h) System vulnerability, (i) Confidentiality, (j) Access Control. This study conducted the Grey Relational Analysis (GRA) to identify the risk factors of the cultural creative IoT and the relative weights of each factors.

Methods

The possible risk factors were derived first from the literature and experts' opinions and then were evaluated by subject matter experts (SME). The SMEs (N = 10) were selected by purposive sampling of people who were managers or related experts using IoT in cultural creative industry. Purposive sampling is mainly used for opinion surveys. For this study, participants were required have been in the cultural creative industry for at least 10 years.

The questionnaire addresses the characteristics of risk factors, using 10 items of responds to the rising security risks of IoT. The answers are constructed with the five point Likert scale. The interviews protocol was developed in English and based on the literature review. The interviews explored more fully the perceptions of the people of experience about theIot in cultural creative industry. Interviews were conducted in Chinese. The codes and supporting words emerging from the transcripts of interviews were translated into English for analyzing.

The grey system method, as developed by Deng [31], has been extensively applied in various fields, including decision science. In this study, the GRA is applied to construct an evaluation method for ranking the risk factors of Iot in cultural creative industry. The GRA is calculated as follows:

LetX_0be the referential series with *k* entities (or criteria) ofX_1, X_2, …,X_i, …, X_N(or *N*measurement criteria). Then

$$X_0 = \{x_0(1),\ x_0(2),\ ...,\ x_0(j),\ ...,\ x_0(k)\},$$

$$X_1 = \{x_1(1),\ x_1(2),\ ...,\ x_1(j),\ ...,\ x_1(k)\},$$

$$\vdots$$

$$X_i = \{x_i(1),\ x_i(2),\ ...,\ x_i(j),\ ...,\ x_i(k)\},$$

$$\vdots$$

$$X_N = \{x_N(1),\ x_N(2),\ ...,\ x_N(j),\ ...,\ x_N(k)\}.$$

ThenThe grey relational coefficient between the compared series X_i and the referential series of X_0 at the j-th entity is defined as

$$\gamma_{0i}(j) = \frac{\Delta\min + \Delta\max}{\Delta_{0j}(j) + \Delta\max}, \qquad (1)$$

where $\Delta_{0j}(j)$ denotes the absolute value of difference between X_0 and X_i at the j -th entity, that is

$$\Delta_{0j}(j) = \left|x_0(j) - x_i(j)\right|, \text{ and } \Delta\max = \max_i \max_j \Delta_{0j}(j),\ \Delta\min = \min_i \min_j \Delta_{0j}(j).$$

The grey relational grade (GRG) for a series of X_i can be expressed as

$$\Gamma_{0i} = \sum_{j=1}^{K} w_j \gamma_{0i}(j), \qquad (2)$$

Where $w_j$represents the weight of j-th entity. If the weight does not need to be applied, take $\omega_j = \frac{1}{K}$ for averaging.

The grey Before calculating the grey relation coefficients, the data series can be treated based on the following three kinds of situation and the linearity of data normalization to avoid distorting the normalized data. They are:

1. Upper-bound effectiveness measuring (i.e., larger-the-better)

$$x_i^*(j) = \frac{x_i(j) - \min_j x_i(j)}{\max_j x_i(j) - \min_j x_i(j)}, \qquad (3)$$

where $\max_j x_i(j)$ is the maximum value of entity$j$ and $\min_j x_j(j)$ is the minimum value of entity$j$.

2. Lower-bound effectiveness measuring (i.e., smaller-the-better)

$$x_i^*(j) = \frac{\max_j x_i(j) - x_i(j)}{\max_j x_i(j) - \min_j x_i(j)}, \qquad (4)$$

If $\min_j x_i(j) \le x_{ob}(j) \le \max_j x_i(j)$, then $x_i^*(j) = \frac{\left|x_i(j) - x_{ob}(j)\right|}{\max_j x_i(j) - \min_j x_i(j)}$, (5)

If $\max_j x_i(j) \le x_{ob}(j)$, then $x_i^*(j) = \frac{x_i(j) - \min_j x_i(j)}{x_{ob}(j) - \min_j x_i(j)}$, or (6)

If $x_{ob}(j) \le \min_j x_i(j)$, then $x_i^*(j) = \frac{\max_j x_i(j) - x_i(j)}{\max_j x_i(j) - x_{ob}(j)}$. (7)

where$x_{ob}(j)$ is the objective value of entity$j$.

Results and Discussion

Table 1. Questionnaire data of the reactions to the risk factors of IoT in cultural creative industry

	Subject Matter Expert									
Factors	1	2	3	4	5	6	7	8	9	10
Privacy	5	5	5	5	5	4	5	5	5	4
Enforcement	4	5	3	4	3	3	4	5	3	4
Authentication	3	5	5	5	4	4	4	5	4	4
Middleware	4	4	2	5	4	2	3	4	5	2
Burglary	5	5	3	5	3	5	4	4	2	5
Jurisdiction	3	1	4	2	3	2	3	2	2	2
Trust	5	4	5	5	4	5	3	4	5	5
System vulnerability	3	3	3	2	3	4	4	4	2	3
Confidentiality	3	3	2	3	4	2	3	2	4	3
Access Control	5	3	5	5	5	4	5	5	4	5

Calculation of $\Delta_{0j}(j)$ equals the difference between X_0 and X_i .The result is in table 2。

Table 2.The calculation result of $\Delta_{0i}(j)$ of the reactions

	1	2	3	4	5	6	7	8	9	10
Δ_{01}=	0.0000	0.0000	0.0000	0.0000	0.0000	1.0000	0.0000	0.0000	0.0000	1.0000
Δ_{02}=	1.0000	0.0000	2.0000	1.0000	2.0000	2.0000	1.0000	0.0000	2.0000	1.0000
Δ_{03}=	2.0000	0.0000	0.0000	0.0000	1.0000	1.0000	1.0000	0.0000	1.0000	1.0000
Δ_{04}=	1.0000	1.0000	3.0000	0.0000	1.0000	3.0000	2.0000	1.0000	0.0000	3.0000
Δ_{05}=	0.0000	0.0000	2.0000	0.0000	2.0000	0.0000	1.0000	1.0000	3.0000	0.0000
Δ_{06}=	2.0000	4.0000	1.0000	3.0000	2.0000	3.0000	2.0000	3.0000	3.0000	3.0000
Δ_{07}=	0.0000	1.0000	0.0000	0.0000	1.0000	0.0000	2.0000	1.0000	0.0000	0.0000
Δ_{08}=	2.0000	2.0000	2.0000	3.0000	2.0000	1.0000	1.0000	1.0000	3.0000	2.0000
Δ_{09}=	2.0000	2.0000	3.0000	2.0000	1.0000	3.0000	2.0000	3.0000	1.0000	2.0000
Δ_{010}=	0.0000	2.0000	0.0000	0.0000	0.0000	1.0000	0.0000	0.0000	1.0000	0.0000

Employ an application with the linearity of data normalization to avoid distorting the normalized data。The calculation result is in Table 3.

Table 3.The result of the linearity of data normalization

	1	2	3	4	5	6	7	8	9	10
γ_{01}=	1.0000	1.0000	1.0000	1.0000	1.0000	0.6000	1.0000	1.0000	1.0000	0.6000
γ_{02}=	0.6000	1.0000	0.4286	0.6000	0.4286	0.4286	0.6000	1.0000	0.4286	0.6000
γ_{03}=	0.4286	1.0000	1.0000	1.0000	0.6000	0.6000	0.6000	1.0000	0.6000	0.6000
γ_{04}=	0.6000	0.6000	0.3333	1.0000	0.6000	0.3333	0.4286	0.6000	1.0000	0.3333
γ_{05}=	1.0000	1.0000	0.4286	1.0000	0.4286	1.0000	0.6000	0.6000	0.3333	1.0000
γ_{06}=	0.4286	0.2727	0.6000	0.3333	0.4286	0.3333	0.4286	0.3333	0.3333	0.3333
γ_{07}=	1.0000	0.6000	1.0000	1.0000	0.6000	1.0000	0.4286	0.6000	1.0000	1.0000
γ_{08}=	0.4286	0.4286	0.4286	0.3333	0.4286	0.6000	0.6000	0.6000	0.3333	0.4286
γ_{09}=	0.4286	0.4286	0.3333	0.4286	0.6000	0.3333	0.4286	0.3333	0.6000	0.4286
γ_{010}=	1.0000	0.4286	1.0000	1.0000	1.0000	0.6000	1.0000	1.0000	0.6000	1.0000

After calculation, the main impact risk factors of IoT in were decided. The result is in Table 4.

Table 4.Grey relational grade of the risk factors of IoT in cultural creative industry

Side Effects	γ_{0i}
Privacy	0.9200
Enforcement	0.6114
Authentication	0.7429
Middleware	0.5829
Burglary	0.7390
Jurisdiction	0.3825
Trust	0.8229
System vulnerability	0.4610
Confidentiality	0.4343
Access Control	0.8629

Conclusions

Through the process of GRA, the most influencing risk factors of IoT in cultural creative industry selected by the interviewers were "Privacy", "Access Control", and "Trust". In this analysis, the satisfaction of the risk management requirements plays a fundamental role. This high level of heterogeneity, coupled to the wide scale of IoT systems, is expected to magnify the risk of the future environment.

The first impacting risk is "Privacy". The convenience of IoTfacilitating the exchange of goods and services in global supply chain networks has an impact on the privacy of the involved stakeholders. The data transmitted by a given endpoint might not cause any privacy issues on its own. However, when even fragmented data from multiple endpoints is gathered, collated and analysed, it can yield sensitive information. The idea of networking appliances and other objects, even in cultural creative field, is relatively new, especially in terms of the global connectivity and independent data transfer that are central to the IoT. As such, privacy has not been considered in product or gallery design, which can make even everyday domestic objects points of vulnerability. Researchers found the vulnerability in a Wi-Fi-enabled light bulb that allowed them to request its Wi-Fi credentials and use those credentials to get network access.Therefore, IoT security needs to be taken seriously, particularly before cultural creative businesses start to connect mission critical devices and systems.

The second consideration is access control. Access control in this new situation is a expanding and challenging problem. An access control system should be broad enough to cover the requirements of all the new exciting applications that become persistent with the IoT. On the other hand, an access control system should be lightweight and easily implementable, considering at the same time the restrictions that each component imposes. That means that access control is also growing in importance. Big data comes from a wide variety of sources and is accessed along many different network vectors and locations along the way. From the initial access sources sent out on the network to the storage array holding it to the analytics platform and end user munching the numbers, big data and the IoT translate into new ways for critical information to leak. Personal information management and access controls must be simple, enforced, and strengthened in order to keep our future of cloud big data platforms intact.

The third risk factor is Trust. Trust is a complex notion about whichno definitive consensus exists in the previous literature,although its importance is widely recognized. A mainproblem with many approaches towards trust definitionis that they do not lend themselves to the establishmentof assessment methodologies.While focusing on trust level assessment of IoTentities,it is assumed that most smart objects arehuman-carried or human-related devices, so they are oftenexposed to public areas and communicate through wireless,hence vulnerable to malicious attacks. Smart objectshave heterogeneous features and need to cooperativelywork together. The social relationships considered are:friendship, ownership and community, since users arefriends among themselves, users ownthe devices (i.e., ownership) and the devices belong tosome communities (i.e., community). Malicious nodesaim at breaking the basic functionality of IoT by means oftrust related attacks: self-promoting, or bad-mouthing. Scientists make an attempt to design anattack-resistant trust management model for distributedrouting strategy in IoT. Such a model can evaluate andpropagate reputation in distributed routing systems andit is then proposed to establish reliable trust relationsbetween self-organized nodes and defeat possible attacksin IoTsystems.

IoT security risks, especially in cultural creative business, still need to face many potential challenges. Besides technique challenges mentioned above, legislative and management issues such as jurisdiction, confidentiality, personal information, are also new challenges to construct a healthy IoTenvironment. All those future research directions and much more derivative new problems will keep immerging in the IoTworld; the whole society should be alerted on these problems.

References

[1]A, Nordrum, Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. IEEE. 18 August (2016).

[2]Y, Erlich, A vision for ubiquitous sequencing. Genome Research. 25 (10): 1411–1416 (2015).

[3]I, Wigmore, Internet of Things (IoT). TechTarget.June (2014).

[4]C. Hsu, J. Lin, An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives". Computers in Human Behavior. 62: 516–527 (2016).

[5]K, Thompson, B. Mattalo,. The Internet of Things: Guidance, Regulation and the Canadian Approach. CyberLex. 24 November (2015).

[6]T, Lane, The "Only" Coke Machine on the Internet. Carnegie Mellon University. Retrieved 10 May, 2018.

[7]F. Palermo, Internet of Things Done Wrong Stifles Innovation. Information Week. 7 July (2014).

[8]R. Raji, Smart networks for control. IEEE Spectrum. June (1994).

[9]P. Magrassi, Why a Universal RFID Infrastructure Would Be a Good Thing. Gartner research report G00106518. 2 May (2002).

[10]P.Day, Peter Day's World of Business. BBC World Service. BBC. Retrieved 13 May 2018.

[11]K, Lewis, The First Thinking Sculpture: Inspired by Gaudi, created with Watson. Mobile World Congress 2017. https://www.ibm.com/blogs/internet-of-things/first-thinking-sculpture/ February 28 (2017). Retrieved 13 May 2018.

[12]J. Clark, IoT and the Arts: Galleries and smart sculptures. Mobile World Congress 2017. https://www.ibm.com/blogs/internet-of-things/iot-arts-galleries/ February 28, (2017). Retrieved 13 May 2018.

[13]I. Lopatovska, K. Rink, Ian Knight, Kieran Raines, Kevin Cosenza, Harriet Williams, Perachya Sorsche, David Hirsch, Qi Li, Adrianna Martinez. Talk to me: Exploring user interactions with the Amazon Alexa. Journal of Librarianship and Information Science. March 7 (2018).

[14]Ali Dorri ; Salil S. Kanhere ; Raja Jurdak ; Praveen Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home, 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, March (2017).

[15]J. Yang, B. Fang, Security model and key technologies for the internet of things, J. China Universities Posts Telecommun. 8 (2) 109–112 (2011).

[16]M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A. Sadeghi, S. Tarkoma, IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT, ICDCS, June 2017.

[17]S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello, A. Coen-Porisini, Security policy enforcement for networked smart objects, Computer Networks, 108(24), 133-147 (2016).

[18]Y. Zhao, Research on data security technology in internet of things, 2013 2nd International Conference on Mechatronics and Control Engineering, ICMCE 2013, Dalian, China, pp. 1752–1755 (2013).

[19]P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, M. Ylianttila, Two-phase authentication protocol for wireless sensor networks in distributed IoT applications, WCNC, April (2014).

[20]Z. Ji, I. Ganchev, M. O'Droma, L Zhao,X. Zhang, A Cloud-Based Car Parking Middleware for IoT-Based Smart Cities: Design and Implementation, Sensors, 14(12), 22372-22393 (2014).

[21]A. Ngu, M. Gutierrez, V. Metsis, S. Nepal, Q. Z. Sheng, IoT Middleware: A Survey on Issues and Enabling Technologies, IEEE Internet of Things Journal, 4(1), 1-20, (2017).

[22]S. Sadhukhan, A. Acharyya, R. Prasad, Car Security System using Fingerprint Scanner and IOT, Indian Journal of Science & Technology, 10(40), (2017).

[23]S. Paquette, P.T. Jaeger, S.C. Wilson, Identifying the Security Risks Associated with Governmental Use of Cloud Computing, Government Information Quarterly. 27, 245-53 (2010).

[24]K. Kalyani, Implementation of IOT in E-Commerce. International Journal of Scientific Research in Science and Technology, 3(8), (2017).

[25]Z. Yan, P. Zhang, A.Vasilakos, A survey on trust management for Internet of Things, Journal of Network and Computer Applications, 42, 120-134 (2014).

[26]D. Chen, G. Chang, D. Sun, J. Li, J. Jia, X. Wang, TRM-IoT: A Trust Management ModelBased on Fuzzy Reputation for Internet of Things, ComSIS. 8(4), 1207-1228, (2011).

[27]J. Casale, Social Networking, Cloud Computing Bring New Risk Exposures, Business Insurance. 44(38), 17,(2010).

[28]S. Alam, M. Chowdhury, J. Noll, Interoperability of Security-Enabled Internet of Things, Wireless Pers Commun. 61(3), 567–586 (2011).

[29]D. He, S. Zeadally, An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography, IEEE Internet of Things Journal, 2 (1), 72–83 (2014).

[30]S.Sicaria, A.Rizzardia, L.Griecob, A.Coen-Porisini, Security, privacy and trust in Internet of Things: The road ahead, Computer Networks, 76 (15), 146-164 (2015).

[31]J. Deng, Grey System Theory and Applications, Lao-Li, Taiwan, (1999).