Authentication Link: A Novel Authentication Architecture in IoT/IoB Environment

Gi-Yoon Jeon

***Abstract*—The authentication is the process of determining whether someone or something is, and there are many authentication methods for digital environment. The digital authentication is divided into three main categories, 'What you have', 'What you know', and 'Who you are'. Furthermore, there are multi-factor authentications using a combination of two or more of these. However, these methods are always exposed to the risk of forgery, tampering, and stealing. This paper proposes a novel authentication architecture that is suitable for Internet of Things (IoT) and Internet of Behaviors (IoB) environment. In the aspect of technology, the proposed architecture is token based authentication method. However, this architecture is continuous, mimics real analog world, and has the advantage of being immediately recognizable in counterfeiting.**

***Index Terms*—Authentication, Authentication Link, Authentication Token, Internet of Things (IoT), Internet of Behaviors (IoB).**

I. Introduction

THE AUTHENTICATION is the process of determining whether someone or something is [1]. There are many authentication methods for digital systems. The digital authentication is verifying a someone or something to allow access to data or systems and that is divided into three main categories, 'What you have', 'What you know', and 'Who you are' [2]. The knowledge factor is 'What you know'. This approaches such as ID and password are low-reliability method because password can be lost, stolen, or guessed [3]. The ownership factor is 'What you have'. This approaches such as ID card can be stolen. The inference factor is 'Who you are', in other words biometrics. This approaches such as finger print, retina requires specialized equipment and have malfunction [4]. Furthermore, there are multi-factor authentications using a combination of two [5]–[7] or more of these [8], [9]. However, these methods are always exposed to the risk of forgery, tampering, and stealing.

The main advantage of IoT is that everything could be connected to a network and communicate each other. However, as a result, the security threat also increases in a very diverse IoT environment, and countermeasures to compensate for it are needed. [10], [11].

The proposed authentication architecture supports a human-to-device communication and also device-to-device communication technology [14].

J. Ma et al [15] and D. Sahraoui et al [16] define an each identities for real world and cyber space, and the relation of identities between real world and cyber space is organized [17]. However, the proposed Authentication Link dose not discrete the real world and cyber space. Rather than the Authentication Link combines the identities by continuous authentication in IoT networks.

What's even worse is that in many cases the digital crime is not reveal. The major reason is that there is enough time gap between the previous authentication and the next authentication. In this paper, a novel authentication architecture using token is proposed for IoT and IoB environment. This Authentication Link is continuous and has the advantage of being immediately recognizable in counterfeiting.

II. Authentication Link

A. Main Ideas

The proposed Authentication Link is originated from the philosophical consideration of existence. All objects, including human beings, can exist only in one place at a time. However, the all actual objects are the results of its past and interaction with surrounding other objects. The identity of an object is in its final existence itself. Obviously the existence of an actual object is equivalent to the past object and its concerned interactions. Therefore, to prove the identity of present object, it is enough to show that the shortly past object and the interactions with the surrounding environment were correct.

In Eq.(1), the letter S is a person or an object to authenticate, and the letter t is time stamp. The time stamp interval could be very short or could have some duration. The letter O_1, O_2, and O_n are the surrounding objects of a person or an object for authentication. The operator $\odot$ means interaction between both operands.

$$S_t \odot O_{1_t} + S_t \odot O_{2_t} + \cdots + S_t \odot O_{n_t} \rightarrow S_{t+1}. \quad (1)$$

therefore, when the time index is adjusted, it can be expressed by the following equation.

$$S_t = S_{t-1} \odot \sum_{i=1}^{n} O_{i_{t-1}}. \quad (2)$$

Obviously, there are interactions between objects, but the Eq.(1) and (2) are described an identity for a person or a specific object represented by letter S. Based on the above Eq.(1) and (2), additional inferences can be possible that if we know the past state of someone(S_{t-1}) and state of all surrounding objects($O_{t_1}, O_{t_2}, \cdots, O_{t_n}$), the present and future state of a person can be accurately derived. And also in the same way, if we know the present state(S_t) of someone exactly, we can excavate the past states of someone and all surrounding objects accurately.

Gi-Yoon Jeon is with the Agency for Defense Development, Seoul, Korea e-mail: melong96@gmail.com

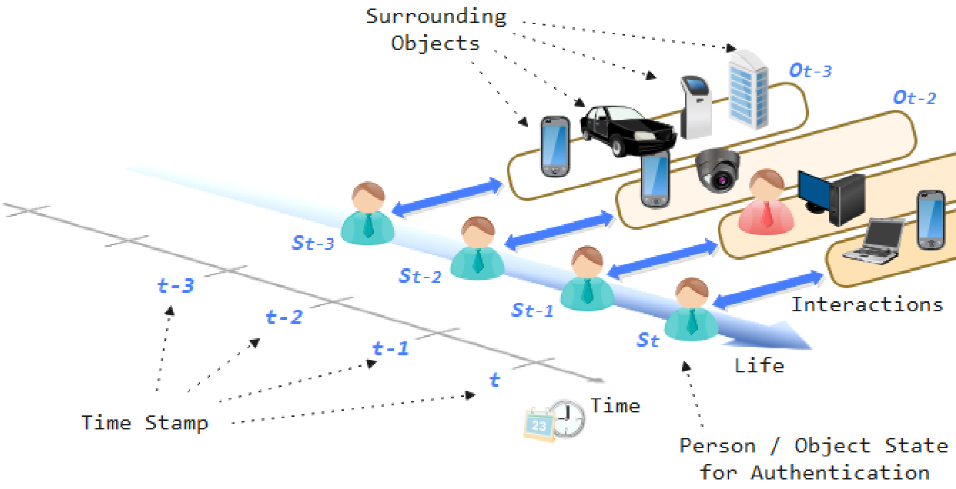

Fig. 1. The states of existence, surrounding objects, and time

The Fig.1 shows the examples of real life and interactions with surrounding objects. At $t-3$ time, the S_{t-3} state person interacted with O_{t-3} objects(a mobile phone, a car, a parking system and a building). The results of these interactions and the S_{t-3} state person formed the S_{t-2} state person. Regarding this, in order to confirm the existence of S_{t-2} state person, it is sufficient to show that the existence of S_{t-3} and its interactions are correct. At the same way, the last or present S_t state person is formed from S_{t-1} and interactions of O_{t-1} objects. These are routine and continuous. When the time stamp interval is wide, the interaction objects would be increased, and when the interval is narrow, the interaction objects would be reduced.

B. *Operational Concept*

Theoretically, as shown in the Eq.2 and the Fig.1, all past interactions should be verified, but the Authentication Link architecture in IoT/IoB environment proposes to verify only one past interaction. The verification of multiple past interactions leads to increase network traffic and complex protocols in the IoT/IoB environment. However, multiple past interactions could be taken into account for higher level authentication implementations, or against an anomaly for only one interaction.

The Fig.2 originated from [9], [12], [13] shows the IoT environment for the Authentication Link. Here are some scenarios for identity authentication. When an Authentication Link user returns home, home security requests the user's identity from the means of transportation, either a car or a public transportation, or a payment machine of the grocery store that is used credit card to stop by on the way home from work. After that, when the user wants to watch a movie using a home theater, the authentication system of the home theater in a login procedure requests home security to verify the user identity.

The authentication link has a contextual connection between present authentication and past authentication. In the same way, the past is connected with more past. Going back, the first authentication is required, which was issued by the certificate authority in off-line. The first authentication is can be abrogated and reissued for appropriate reasons.

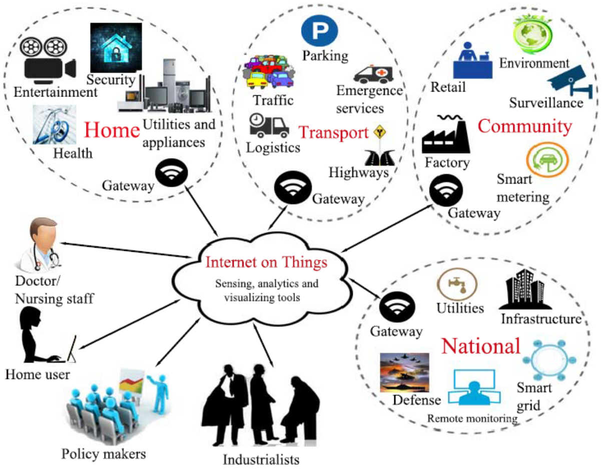

Fig. 2. IoT Environment [9], [12], [13]

C. *Operational Procedures*

The Fig.3 shows the authentication sequences for some user. The payment machine images are used, but the all IoT devices can be such as mobile phone, personal computers, parking systems or other public services. The blue colored procedures(②ID Validation Request, ⑤PIN) are optional. The operational procedures are explained based on the Fig.3.

1) *Connecting:* The user connects an IoT device for some service with token that was created from past IoT device. The token contains 'User ID', past token generation IoT 'Device Address', token generation 'Time', and 'Token ID' at time t from past IoT device.

2) *ID validation requesting:* The present IoT device reads the contents of token, and requests the current user identity validation to the past IoT device using the 'Device Address'.

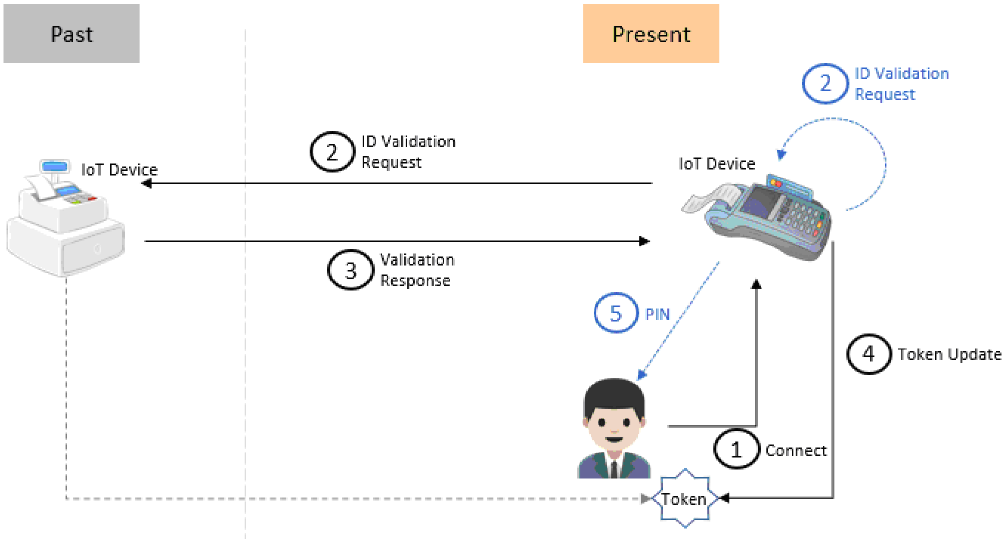

Fig. 3. Operational concept diagram

The validation request message includes the 'User ID', 'Time', and 'Token'. As the Fig.3, the blue colored ②ID Validation Request can be occurred when the user contacts the same device after some service, or the duration of service is long enough at the same device with the ④Token Update procedure.

3) Validation Reporting: The past device maintain a validation list for reporting to the validation request of present device. There are three kinds of validation responses. The first is 'Valid', the second is 'Invalid', and the last is 'Time out'. The validation function and validation list management will be described at the Sec.II-D and the Sec.II-E each.

4) Token Updating: When a service is terminated or a service time is long enough, the 'Token Update' procedure is occurred. The present device changes the 'Device Address' from past device address to the own address and generates a new 'token ID' at time t. The 'Time' is time used for token generation. The token generation function will be described at Sec.II-D.

5) PIN Issuing: This is optional or alternative procedure. When a user want to adapt a multi-factor authentication, and there is a suitable input facility at the authentication IoT devices, the PIN can be issued. If the IoT network is broken, this PIN can be used for user authentication like a basic token-based authentication.

D. Token Structure

The Authentication Link is token-based method. The Table I shows the data elements for the Authentication Link token.

1) User ID: The user ID and first token could be issued by certificate authority only. The user ID can be incremental integer number or like a common user ID for internet portal site. An user e-mail address is also possible.

2) Device Address and Device ID: The 'Device Address' is network address like as IP address. The present device is able to send a validation request message to the past device using this 'Device Address' in Authentication Link network. When the present device generates a 'Token' at time t, the 'Device Address' is updated to the present device address. In the Authentication Link, the IoT devices are participants as an operator for authentication. The 'Device ID' is defined for the each Authentication Link network and this ID should not be opened to public for security. This 'Device ID' is unique at a network like as MAC address, and stored in the device only. The token generation function(tgf, see Eq.3) uses the 'Device ID' for token generation.

TABLE I
THE DATA ELEMENTS OF ACCESS TOKEN AT TIME t

1	User ID	The number of user generated from certificate authority
2	Device Address	The previous device network address who creates the T_t value at time t
3	Time	Token generation time at time t
4	Token$_t$	The token ID value for access token at time t
5	PIN$_t$	Optional number, one time personal identity number at time t

3) Time: The 'Time' is time when the 'Token' generated and it can be a UNIX or UTC time. It depends on the Authentication Link network design and this is also used for token generation function(tgf, see Eq.3). Because of the 'Time' value generation and the validation conduct at the same device, the device does not need time synchronization for Authentication Link network.

4) Token: The token is the value that determines whether the user's identity is valid or not for the device that requested authentication. The token is generated by token generation function(tgf, see Eq.3), and this is a kind of hash function. The token length and hash method are the Authentication Link design matters. There are three input parameters for tgf. The 'User ID' and 'Time' are stored in token structure, but the 'Device ID' is only stored in the Authentication Link device each. The operator $\oplus$ is a set of binary operations for making a input value to tgf with 'User ID', 'Device ID', and 'Time' in Eq.3.

$$\text{Token}_t = tgf(\text{User ID} \oplus \text{Device ID} \oplus \text{Time}). \tag{3}$$

5) Optional PIN: The Authentication Link users can adapt a PIN(Personal Identity Number) to their token optionally. This is an additional function to use a more secure multi-factor technique, or alternatively, it can operate like pure token-based authentication in the event of disconnection or failure of Authentication Link network. When a user ask a PIN, the token generation IoT device should be able to issue PIN, and token validation IoT device should have input facility for the PIN and verify its validity. If this PIN is used only for authentication without Authentication Link, and when the network is restored to normal, a additional procedure should be considered for notifying the previous device that the user has been authenticated using the PIN.

E. Validation List

When an IoT device participates in Authentication Link, it receives a 'Device ID', and the participant device could create and manage a Validation List for authentication. The token generation devices are responsible for responding to an authentication request. The Table II shows an instance of validation list for the Authentication Link at a time. The pair of 'User ID' and 'Time' is key value.

When a new user connects to an Authentication Link device, the present device requests the authentication of new user to the past device. After this authentication process, present device generates a token and inserts 'User ID', 'Time', and 'Request' record to Validation List. The first 'Request' value is '0'. It means there is no request authentication for this user yet. When this user connects other device, the other device will request authentication for this user, and then the 'Request' value is updated to '1'. If there are another authentication request from some devices, it means the token for this user is copied or tampered illegally. In this case, the 'Invalid' response is transmitted to the device. In accordance with this violation, this status should be notified to the user and Authentication Link network depending on network design. When the 'Request' value is '2' and there are additional authentication requests, it is also possible to accumulate a 'Request' value of '3' or more.

Because Validation List cannot be maintained indefinitely, each record could be deleted after a certain period of time. There are three cases of record deletion by time-out, and each time-out setting value is also an Authentication Link design matter. The Fig. 4 is a flow diagram for Validation List maintenance.

TABLE II
AN EXAMPLE OF VALIDATION LIST

User ID	Time	Request	Remark
⋮	⋮	⋮	⋮
user001	1589158900	2	copied
user002	1589158959	1	ID requested
user002	1589158999	0	ID unrequested
⋮	⋮	⋮	⋮

F. The characteristics of Authentication Link

The Authentication Link is token based authentication method. However, compared to the existing pure token based

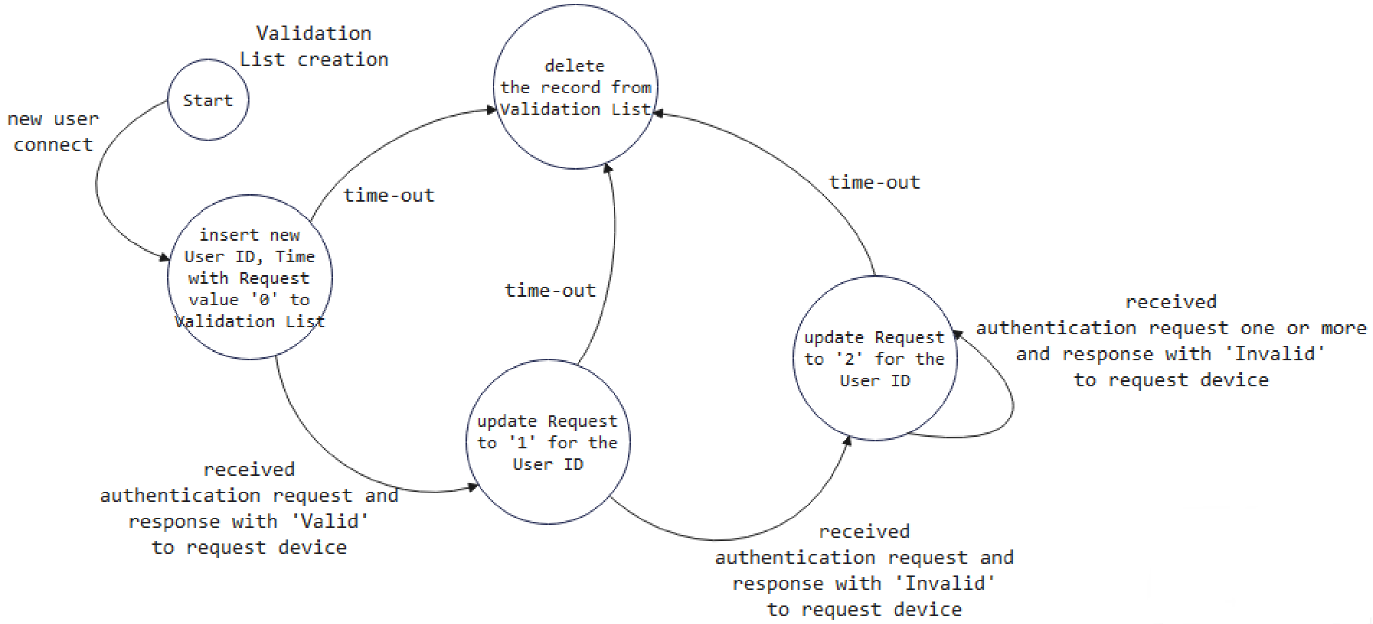

Fig. 4. The Flow Diagram for Validation List Management

authentication method, the Authentication Link has several characteristics.

1) A series of authentications consist a link: Like the Eq. 1 and 2, the present state of someone through the authentication link is based on the past authentication. Therefore, the each authentication is defined recursively and logically relies on initial certificate authority.

2) Sensitive to copying or tempering: There is a possibility that a token might be copied or tampered with by a malicious IoT device or user's negligence. However, through the Authentication Link procedures and Validation List management, the Authentication Link network and user could immediately recognize illegal token copying or tampering.

3) IoT authentication system: In an environment where a server is a participant of an Authentication Link, it could be implemented for a client-server architecture. However, the main point is that the proposed architecture is conducted between IoT devices. It makes an IoT device of a subject of authentication, and could be an conceptual basis that a network is an authentication system.

III. Issues to Overcome

The authentication link is novel and human friendly architecture, nevertheless there are some challenges to solve some issues due to the limitations of IoT network. Above all, IoT devices have low processing performance, small memory size, and small battery capacity. In the Authentication Link, the network traffic would become very large. This causes techniques to reduce network traffic and battery consumption [18]. Also, there is an issue of communication security between IoT devices. However, this security problem is resolved by communication security method, like a cryptography and this issue is out of scope in this proposal.

When a sudden situation such as token tempering occurs in the Authentication Link, a exceptional process is needed to notify the entire network and prevent the tempered token from being used any more. Similarly, if someone wants to no longer use Authentication Link, who declares to the IoT networks. Also, to start a new Authentication Link service, the first token should be created with off-line certificate authority, which can cause inconvenience to users.

IV. Conclusion

The digital authentication is very important in IoT/IoB environment, and this proposed authentication architecture is suitable for IoT/IoB environments. Furthermore, this architecture could be applied to other general networks or authentication systems.

As prophesied by 'Being Digital' [19], it seemed that everything would be expressed and processed in digital. However, the analogue persists. The metaverse and NFT(Non-Fungible Token) are examples of efforts to implement analogue in a digital environment. The Authentication Link is also based on analogical concept. Digital would never stop admiring analogue and try to be the same forever with bigger data and higher performance systems.

References

[1] E. McTigue, E. Thorton, and P. Wiese, "Authentication projects for historical fiction: Do you believe it?" *The Reading Teacher*, vol. 66, issue. 6, pp. 495–505, 2013.

[2] A. C. Weaver, "Biometric authentication," *Computer*, vol. 39, issue. 2, pp. 96–97, 2006.

[3] S. Egelman, S. Jain, S. Portnoff, K. Liao, S. Consolvo, and D. Wagner, "Are yout ready to lock?" *Proc. 2014 ACM SIGSAC Conf. Computer and Communications Security*, pp. 750–761, 2014.

[4] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Processing Magazine*, vol. 32, issue. 5, pp. 54–65, 2015.

[5] M. H. Eldefrawy, k. Alghathbar, and M. K. Khan, "OTP-based two-factor authentication using mobile phone," *2011 8th International Conference on Information Technology: New Generations*, pp. 327–331, 2011.

[6] D. P. Roberto, M. Gianluigi, and S. M. Adriano, "A two-factor mobile authentication scheme for secure financial transactions," *IEEE International Conference on Mobile Business*, pp. 28–34, 2005.

[7] M. A. Crossman, and H. Liu, "Two-factor authentication through near field communication," *IEEE Symposium on Technologies for Homeland Security*, pp. 1–5, 2016.

[8] P. Shen Teh, N. Zhang, A. Beng Jin Reoh, and K. Chen, "TDAS: a touch dynamics based multi-factor authentication solution for mobile devices," *International Journal of Pervasive Computing and Communications*, vol. 12, issue 1, pp. 127–153, 2016.

[9] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet of Things*, vol. 5, no. 1, pp. 269–282, 2018.

[10] M. Qayyum, and M. Husamuddim, "Internet of Things: A study on security and privacy threats," *2017 2nd International Conference on Anti-Cyber Crimes(ICACC)*, pp. 93–97, 2017.

[11] T. A. Ahanger, and A. Aljumah, "Internet of Things: A comprehensive study of security issues and defense mechanisms," *IEEE Access*, vol. 7, pp. 11020–11028, 2019.

[12] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things(IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[13] S. Challa, M. Wizad, A. M. Das, N. Kumar, A. G. Reddy, E. Yoon, and K. Yoo, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[14] Z. Yan, H. Xie, P. Zhang, and B. B. Gupta, "Flexible data access control in D2D communications," *Future Generation Computer Systems*, 2017, doi: 10.1016/j.future.2017.08.052.

[15] J. Ma, H. Ning, R. Huang, H. Liu, L. T. Yang, J. Chen, and G. Min, "Cybermatics: A holistic field for systematic study of cyber-enabled new worlds," *IEEE Access*, vol. 3, pp. 2270–2280, 2015.

[16] D. Sahraoui, H. Ning, C. Shan, J. Ma, R. Huang, and K. I. Wang, "Cyberentity and its consistency in the cyber-physical-social-thinking hyperspace," *Computers and Electrical Engineering*, vol. 81, no. 106506, 2020.

[17] H. Ning, Z. Zhen, F. Shi, and M. Daneshmand, "A survey of identity modeling and identity addressing in Internet of Things," *IEEE Internet of Things*, vol. 7, no. 6, pp. 4697–4710, 2020.

[18] Z. Zhao, M. Min, W. Gao, Y. Wu, H. Duan, and Q. Ni, "Deploying Edge Computing Nodes for Large-Scale IoT: A Diversity Aware Approach," *IEEE Internet of Things*, vol. 5, no. 5, pp. 3606–3614, 2018.

[19] N. Negroponte, *Being Digital*, USA: Alfred A. Knopf, Inc., 1995.