A Cloud Based Conceptual Identity Management Model for Secured Internet of Things Operation

Abubakar Bello[1,*] and Venkatesh Mahadevan[2]

[1]*Western Sydney University, Penrith, NSW 2751, Australia*
[2]*Melbourne Institute of Technology, Melbourne, VIC 3000, Australia*
E-mail: a.bello@westernsydney.edu.au
[*]*Corresponding Author*

Received 11 July 2018; Accepted 24 September 2018;
Publication 29 October 2018

Abstract

An era ago, projecting artificial intelligence as the pillar of next-generation technology would have been technically difficult. Today, machines are getting smarter, sparking a new wave of technology that resulted to Internet of Things (IoT). With IoT in play, individuals are able to connect more electronic devices other than smartphones and computers to the Internet. The vision is to create the possibility to manage electronic appliances via the Internet with the most minimal human intervention. IoT promises the application of computing to anything anywhere, and anyone at any time. Thus, it has been estimated that over 100 billion devices will be running the IoT model – drawing the power of cloud processing to create a massive network of devices that are bound to change the essential facets of life in various dimensions. However, several obstacles remain to fulfill this vision, among them is security concerns from an Identity of Things (IDoT) management perspective. IoT devices and users are already under cyber attacks, and any lapse in identity management will propagate these attacks. This paper examined how identity management for IoT is likely to play out in a world where the Internet and cloud technologies are expected to take center stage in the running of day-to-day activities. The paper analyses the identity of things challenges in IoT, followed by a proposal of cloud identity management model for IoT.

Journal of Cyber Security and Mobility, Vol. 8_1, 53–74. *River Publishers*
doi: 10.13052/jcsm2245-1439.813

Keywords: Internet of Things, IoT Security, Identity of Things, Cloud IoT, Identity Management.

1 Introduction

The Internet is awash with legal and illegal activities. Subsequently, Internet of Things (IoT) has to be approached from an angle that supports security. Atzori, et al. [1] described IoT as the inter-connection of diverse networked entities that embrace various forms of communication. Therefore, security parameters for IoT are expected to take a different twist because other than Human-to-Machine (H2M) operations; the machines will also be able to communicate to each other without human intervention using Machine-to-Machine (M2M) communication models [2]. M2M technology has already been in use on a vast scale as mobile communication devices can connect and interchange information with the help of telecommunication networks such as GSM, 3G, 4G, and other wireless technologies like Wi-Fi, RFID, Bluetooth, Bluetooth Low Energy and Dedicated Short Range Communication (DSRC) technologies. These connection techniques allowed developments of computational nodes, sensors, actuators, and receivers for IoT devices to connect and exchange data [3]. For instance, let's consider a situation where a sensor device in a server room amasses data on heat and moisture. The accumulated data by the sensor is then sent to a processing node for decision making where the actuator receives a control signal to manage the HVAC heating/air-conditioning system. A simplified working principle of this IoT concept is represented in Figure 1 below.

Although the operational concept of IoT seems alluring as illustrated in Figure 1, its adoption can be weak without adequate security considerations. It is apparent that IoT's security constraints will need to uphold confidentiality, integrity and authentication features which are significant for various reasons. One of which is the fact that a "thing" goes through various stages, therefore, its security architecture may vary from one stage to the next during the "things" lifecycle. Additionally, since the manufacturing stages of IoT components can have different security protocols embedded, owing to the fact that some security nodes must be created by the manufacturer [4], this can make IoT security controls challenging to craft. Product counterfeiters can also clone the products and use them to gather sensitive details from unsuspecting beneficiaries of IoT operations [5]. Morgan [6] and O'Neill [4] noted that security developers and cyber security experts are in search of practical ways

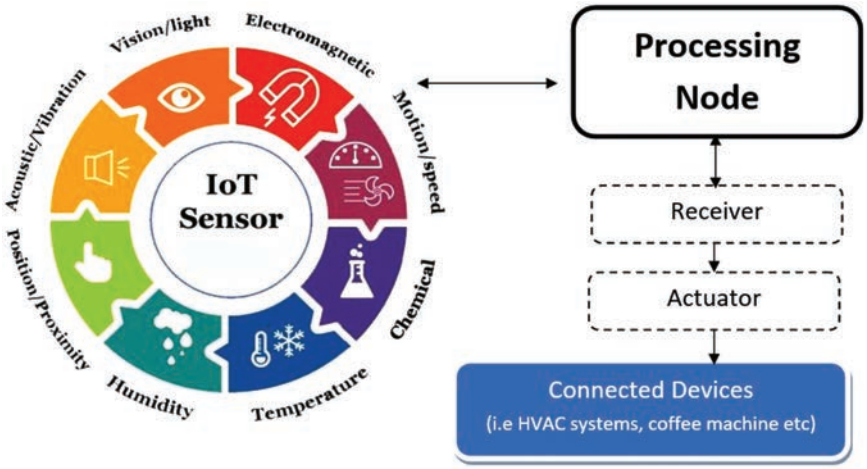

Figure 1 Operational principle of IoT.

to carve out IoT-security parameters to avert some of these challenges using centralised security systems, where the central entity will be densely encrypted and employ technologies such as 6LoWPAN/CoRE – a combination of the latest version of the Internet Protocol (IPv6) and Low-power Wireless Personal Area Networks (LoWPAN) [7]. However, a centralised security system may not augur well with low power appliances and neither will they be able to offer excellent services in areas with poor connectivity [8].

A significant amount of work on authentication protocols for IoT has also been undertaken by many vendors and researchers [9–11]. These are based on numerous algorithmic Internet protocols that allow for reliable access configurations. IoT users can switch lights on/off at home, office or while on vacation half-way around the world by authenticating themselves via a security mainframe with the help of protocols such as: Protocol for Carrying Authentication for Network Access (PANA). This UDP-based protocol at the network layer makes use of the Extensible Authentication Protocol (EAP) – a two-party security protocol that generates digital keys needed for user access and management of a specific home or office appliance [12]. According to Black and McGrew [13], the authentication nodes rely on Host Identity Protocol (HIP) or the Internet Key Exchange version 2 (IKEv2) technologies to ensure that only permitted persons gain access to the control environment. Smaller products with low-energy storage capacity can have their connection models based on Diet-HIP [14]. This protocol version is designed to reduce

the amount of energy that is required for computation as well as encryption and decryption of data – paving the way for even some of the smallest devices such as toothbrush and shaving machines to connect to the Internet [15]. All these protocols may seem effective, however, their insecure implementation and lack of advancement to keep up with IoT developments such as cloud-IoT can contribute to the high risk of devices being compromised.

To secure IoT means to control and manage various complications. Existing protection mechanisms such as trivial cryptographic algorithms and secure protocols are not enough. Identity management is another critical issue besetting IoT [16–18]. The objective of IoT is to interface with other objects to communicate, which requires the exact identification of legitimate and illegitimate objects to establish or cancel a communication and action session. Present identification technologies include biometrics, 2D tags, RFID, QR codes etc. However, an overall standardised framework for the identification of things is lacking [19]. As the cloud is becoming the prominent computational processing node for IoT, developing a systematic cloud-IoT identity management framework is more imperative than ever. To begin with, proper analysis and understanding of the risks associated with various independent and dependent elements of IoT for identity management is essential. This paper starts by performing a security analysis of IoT with focus on Identity of Things (IDoT) challenges, followed by exploring the related work and developments on identity provisioning for IoT. The analysis of identity management issues in cloud-IoT is also carried out, and formed the basis for the proposal of a conceptual identity management model. The paper is then concluded with directions for future research.

2 Security Analysis of IoT

IoT claims many benefits such as flexibility, comfort, and efficiency [20]. However, it also has a great potential for disaster if security issues are not highly prioritised. The generic architecture of IoT according to [21], comprises of network, middleware, and application layers which are all susceptible to several types of attacks. These layers and some of their potential attack types are analysed in Table 1 below.

Based on the heterogeneity and the scale of "things" in IoT, such security issues analysed in Table 1 could become more complex due to the challenges of identification of things, and assigning the correct "thing" to the right "service". Hence, the identity of things challenges requires further analysis within the perspective of achieving effective security for IoT.

Table 1 IoT attack types at different IoT layers

Architectural Layers of IoT	Attack Types/Methods
Network layer – consists of the Wireless Sensor Network (WSN) that transfers data from the sensor to its destination (i.e., actuator).	• **Unauthorised access** to the IoT sensors/tags could result to instructional/execution data being modified or deleted, especially given the lack of strong authentication protocols for RFID systems and tags. • **Eavesdropping** to sniff out confidential data (i.e., passwords) flowing from RFID reader to IoT sensor/tag or vice versa. • **Spoofing** as a result of fake broadcast to IoT sensors/tags. • **Sybil attacks** through manipulation of single nodes to have multiple identities. • **DoS attacks** to flood the network with unwanted traffic which could result to resource exhaustion, damage or shutdown. • **Sleep deprivation attack** to minimise the lifetime or exhaust IoT sensors running on battery.
Middleware layer – comprises of data storage technologies such as cloud.	• **Unauthorised revocation of access** for IoT sensors to services. • **Tampering with the integrity** of transmitted or stored data.
Application layer – handles the practical application of IoT based on the different needs of users.	• **Ransomware** to block access to data and IoT services by encrypting them unless a ransom is paid. • **Malicious code injection** to gain full control of the system or in worst case scenario shuts down the complete IoT environment. • **Social engineering/phishing** to deceive users into giving up their IoT credentials.

2.1 Identity of Things (IDoT) Challenges in IoT Environments

The very nature of IoT means easy device detection and manipulation, and using IoT devices' identity and access to facilitate malicious attacks. Although "things" can be easy to detect, their identity remains difficult to establish or compose for different objects, particularly in a multifaceted object to object communication scenarios [22]. Concisely, IoT identity challenges can be said to take two dimensions: Things-to-Things (T2T) and Human-to-Things (H2T). Both of these dimensions must be considered because they either directly or indirectly affect the Identity of Things.

2.1.1 Things-to-Things (T2T) IoT Challenges

IoT would greatly benefit from a T2T identifier since object attributes, behaviour or environment can keep changing. T2T identifier between different vendor products has mainly relied on IP addresses which is a managed process with several complexities of its own. An example of a farming industry scenario reported by Friese, et al. [23] proved such complexity between a harvester and a truck that were unable to communicate due to uncommon infrastructure. Despite both the harvester and the truck having IP-connectivity via mobile LTE/3G network, they were unable to exchange identifiers in the following days when the IP-address changed as a result of IP-address pools used by mobile network operators. Whenever a device accesses a mobile network, it might be assigned a different IP-address, hence this becomes an identity challenge for such IoT case. Furthermore, T2T should not, for example, trigger scenarios that results to home or office appliances wrongly identifying and initiating communications between each other that are not needed [24]. A water heating kettle can for instance trigger communication with the cooker instead of the dishwasher and commence functions on their own if identity management isn't configured correctly or secured against cyber attacks – leading to energy wastage, electric fire incidents, or even ransomware attacks. Similarly, a car's IoT environment can fail to send the required signals to other vehicles due to identification errors, leading to road accidents. These safety and security challenges ought to be considered by identity management designers to prevent dissonance and mismatch of identities that can set the environment of IoT's into disarray [25].

2.1.2 Human-to-Things (H2T) IoT Challenges

H2T challenges facing IoT environments hinges on the countless possibilities of cyber-attacks. Highly automated systems that may integrate online payment options will, for instance, be one of the prime targets for financially motivated cyber criminals. Users wishing to pay utility bills for specific appliances can, in this case, have their payment cards' authenticating protocols intercepted by fraudsters. Eavesdropping combined with traffic analysis can enable an attacker to recover the identity and location of communicating hosts for spoofing attacks. Through effective traffic/packet analysis, attackers can observe the type, frequency, and length of messages being exchanged to identify specific roles and activities assigned to IoT devices. Disrupting access using denial of service attacks could also be inevitable due to most IoT devices having small memory and limited computational resources [26]. This makes them vulnerable to resource and network exhaustion attacks since

attackers can flood several requests to objects for the purpose of depleting their resources such as bandwidth, memory, or processor time; or even breaking down communication channels between nodes.

Aside the numerous authorisation protocols currently in use, and others being developed to ensure that identity and access management for IoT environments are implemented with precision, the above challenges still remain and more underway. Authentication and authorisation credentials needed to identify and operate a specific IoT device should only be available in scenarios that it is required and when it is required [27, 28]. Many IoT vendors and researchers are now focusing their efforts on developing tamper-proof systems using the power of the cloud and sensors that can trigger distress signals for any malfunction scenarios in IoT [29–31]. However, with billions of devices estimated to be connected, this will be difficult to manage without an identity management framework.

3 Related Work

The growing interest in IoT is well exemplified by the number of research initiatives arising worldwide. For the past few years, there are increasing research efforts on tackling object identification, authentication, and management challenges in IoT. Many of these researchers such as [32–34] focused on authentication models based on the assumption that there should be an expected profile of which an IoT object is in [35], and how the object should behave [36, 37]. For example, an IoT object should have an IP address within a predefined range, and both the object and its sensor's geolocation must be within a specific area. This approach relies on the IP address as the identifier. Other identity management techniques that exist within the context of IoT are: URL as an identifier [38], ubiquitous code [39], ODI [40], short OID [41], EPC [42], and RFID object identifier [43]. These identity schemes including the one proposed by Near Field Communications forum have been analysed and their limitations summarised in Table 2.

Furthermore, the authors [44] in their study addressed identity management issues in IoT by proposing naming and addressing schemes. Digital shadowing by means of verifying object ownership and identity was also presented by [45]. Their solution worked on the pretext of using cloud to assign virtual identity to users and things onto nodes. However, only virtual identity representing data was considered, leaving the addressing and implementation protocols unaddressed. The usage of clustering and Wireless Sensor Network (WSN) protocols for effective identity management has

Table 2 IoT identification schemes limitations

IoT Identification Schemes	Limitations
IP address as the identifier	Scalability issues, and may also not be suitable for IoT objects with resource constraints.
URL as an identifier	Lack of flexibility of binding objects to multiple services within different changing locations.
Ubiquitous code	Considered weak due to 128 bit fixed length identifier system and could potentially declare data transferred because of reverse logic of code for reuse.
ODI	Unsuitable for physical IoT objects, and needs supporting infrastructure overload to operate.
Short OID	Similar to RFID OID and can only use meta-identifier for location of IoT objects.
EPC	Some restrictions exist on the number and type of IoT objects/services, and assemblies/groupings that may be uniquely identified.
RFID object identifier	No identity resolution system to address different IoT object ID structures.

also been proposed by [11, 46], but they failed to address the mobility of objects. Many other identity solutions from IoT vendors are focused on the internet domain level and IP networks [44, 47]. Other solutions mainly consider identities of end users such as OpenID [48], Liberty Alliance, and Shibboleth [49] for identification within the IoT environment. User attributes, and authentication provisioning using technologies such as cloud were the key aspects of these solutions with some emphasis on object identity lifecycle and few assumptions on integration of services with identity. This is still lacking any standardisation. In addition, despite the cloud has been leveraged for centralised identity management to exchange authentication information relating to the attributes of end users, and hosting of services, there is still no systematic work that interlocks the modules of object identity and service identity using cloud to aid authentication and authorisation for mapping and ensuring correct accessibility of an object to a service and vice versa is assigned. Addressing this concern will be one of the main contribution of this paper. The following section analyses how cloud-based IoT solutions can attempt to address identity management issues of IoT.

4 Analysis of Cloud Models for Identity Management in IoT

Beltran [50] and Aazam, et al. [16] observed that the most effective identity management systems for IoT should be cloud focused due to the ability to

provide centralised control and management of devices. IoT's reliance on the cloud further stimulated the re-examination of security solutions that are more scalable [51]. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and Back-end as a Service (BaaS) models can allow for automated deployment of identity policies and controls to enable control over things/devices in IoT environment. Figure 2 below illustrates how each of these cloud platforms could potentially support the centralised integration of identity management for IoT on different levels.

IaaS was among the first model that quickly shaped the platform for M2M communication given the security tenets projected in its ability to support voice and data packages. The ingenious connectivity design led to the development of services such as Subscriber Identification Module (SIM) for use in the mobile phone industry [52]. PaaS model, on the other hand, handles more complex computing factions compared to IaaS. It allows for an integrated communication system that includes voice calls, video chats and data storage capabilities [53]. PaaS can also handle semantic identification which is likely to bring a revolution into IoTs' security issues with support from Application Enablement Platform (AEP) [54]. With PaaS, it is possible to gear for a voice-controlled IoT environment making it likely to turn off the alarm system or the refrigerator on and off by just saying the words "start" or "stop".

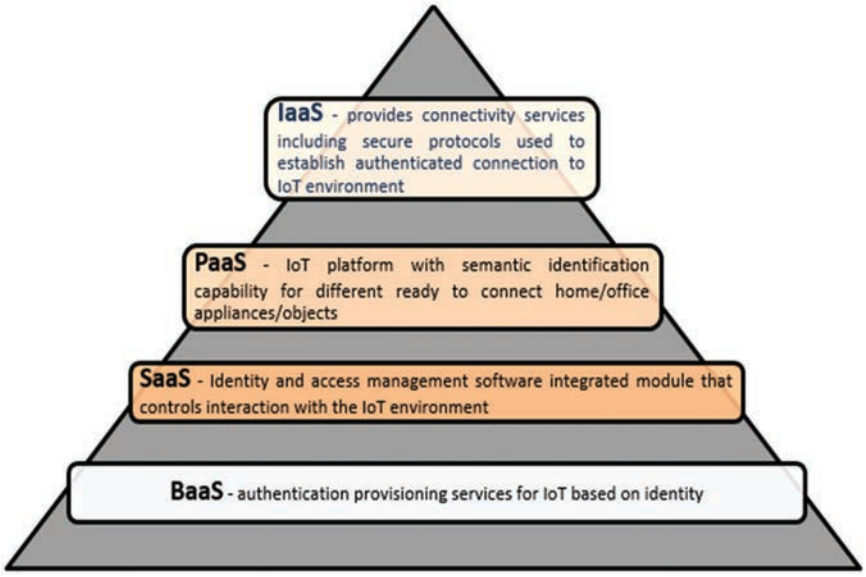

Figure 2 IaaS, PaaS, SaaS and BaaS potential identity control for IoT.

SaaS, is also another model that can be useful in configuring IoT devices because it supports end-to-end integration access and control. It is apparent that SaaS is one of the only systems with the ability to bring together upstream and downstream connectivity for things/devices on both sides of the chain. The result is an increased level of artificial intelligence for the IoT machines – making it possible to implement essential identity and access features with the ability to facilitate a centralised automated control [55]. Another cloud platform with great tendency for identity management control for IoT is BaaS. This platform can be designed to improve the quality of user and device identity protocols and to offer elevated consumer experience concerning access management scenarios for IoT [56]. Its provisioning attributes make it possible for cross-sector operations. IoT vendors may use BaaS to offer their products across the market, bringing down the cost of connection to competing services. From an access control perspective, identity provisioning services can be deployed to ensure that only a genuine device or user with trusted credentials is connected to a specific IoT environment.

Overall, it is important to note that while IaaS, PaaS, SaaS, and BaaS can be reworked to offer some level of identity and access management for IoT, specific gaps existing in each of these individual platforms (reported in Table 3) must be addressed before the integration of additional layers of identity and access controls to their architecture.

As indicated in Table 3, IaaS platforms behave much like physical computers, resulting to greater responsibilities of securing each computing node manually [57]. SaaS does not offer a framework that allows users to gain control of the system's data processing protocols. Software products that run SaaS cannot, for example, be modified to offer better control of identification protocols. Entities that use SaaS are subsequently unable to upgrade their

Table 3 IaaS, PaaS, SaaS, and BaaS IoT gaps

Cloud Platforms	IoT Gaps
IaaS	• Difficulty in securing every aspect of the IoT and its related underlying low-level computing resources such as storage, memory etc.
SaaS	• Provides no control over the infrastructure the IoT applications may run on
PaaS	• Provides no control over the underlying hardware/OS that powers the IoT • Possibility of accessing unencrypted IoT data
BaaS	• Data loss risks due to code restriction risks to block integration of backend programs • Difficulties in testing

operating systems using User Acceptance Testing (UAT) approach [58]. Similar to SaaS, it is possible to access unencrypted data from a PaaS infrastructure [59]. Another gap that exists when using the PaaS model is its inability to protect data because it relies on the less advanced Virtual Machine (VM) data processing systems. Investing in PaaS, therefore, requires one to adopt advanced cloud computing technologies which could also mean bigger chips, bigger power drains, bigger batteries for IoT devices. Thus, raising the cost for both IoT solution providers and individual consumers. To adopt BaaS means the willingness to contend with problems that relate to source code interruption. The reason for this lies in BaaS code restriction measures that it uses to block back-end programs [60]. Its architecture would need to be re-designed to enable reliable identity management in an IoT environment.

Until redevelopments and enhancements are accomplished for IaaS, SaaS, PaaS, and BaaS, identity management for IoT using any of the platforms will be risky to implement. Nevertheless, their current architecture can be leveraged to support the integration and hosting of identity provisioning and data processing services for IoT. This has been considered in the next section of this paper to overhaul the identity management issues discussed in previous sections.

5 Towards a Cloud Approach for Overhauling Identity Management Issues in IoT

To overcome identity management issues in IoT, a staggering variety of principles relating to the connected thing/device itself must be considered. A rule of thumb is that every IoT device should know the identity of other devices it will be interacting with, as well as its owner. For example, devices that monitor and control a user's blood sugar level must know how to precisely identify and relate that information to the device that reports the overall health of that user. Also, a device should be able to identify itself using its specific features while also understanding that its identity is not the same with the identity of its associated mechanisms. For instance, while a device might have an IP-address, it should also have a unique identity of its own to distinguish it from other related integrated systems.

Extending identity provisioning for IoT to the cloud can allow capabilities for better device identity management. The primary idea behind cloud-IoT is to achieve centralised control over how IoT functions by leveraging cloud capabilities for storage and computational power of data processing. As

discussed earlier in the farming truck and harvester scenario, IoT devices may hop from one network to another. In such circumstances, every time a thing/device is operational (refer to Figure 1), it has to send its gathered data to the requesting processing node. With cloud-IoT, rather than issuing commands to other devices, it is best to store the data in the cloud where it can be retrieved when required. The cloud can store large amount of information from various devices making it easy to identify and keep track of every device that data is collected from. The computation power of the cloud can handle the intensive demand of data processing to facilitate decision making from the accumulated data from devices before invoking commands to receivers and actuators. To effectively accomplish these would require an understanding of the relationship between the following actors with roles to play in the cloud, and their relationships in IoT environment.

- "Things/devices" – to collect and transmit data
- "Processing node" – to process data exchanged by things/devices
- "Receiver" – to receive signal instructions/commands from processing node or other things/devices
- "Actuator" – to trigger a thing/device to execute a specific task

The role played by Things/devices would relate to authenticating themselves to the cloud and possessing the relevant authorisation to store information in the cloud. Likewise, the receiver nodes would need authentication to obtain the relevant authorisation to identify as a legitimate receiving entity. Additional authorisation protocols may be needed to ensure receivers/actuators only get data and commands from authorised things or devices. Since data is going to be hosted in the cloud, establishing access controls to disenroll things/devices that may change the membership of their network is crucial. Issues of device identity theft among things and rerouting of data to wrong receivers will also need to be addressed. These aspects are considered in the next section where an identity management framework for IoT is proposed.

6 Conceptual Identity Management Model for IoT

In light of the analysis in the previous sections of this paper, an identity management framework for IoT that leverages cloud capabilities should comprise of two interconnected modules: a "thing/device identity manager", and a "thing/device service manager". The thing/device identity manager would act as a verification segment which confirms the identity of devices, receivers and other computational services hosted in the cloud by

means of authentication. The thing/device service manager will provide the authorisation mechanisms for mapping and ensuring correct accessibility of a device to a cloud-IoT service to the receiver/actuator and vice versa is assigned. An overview of the operational mode of these modules for IoT identity management is represented in Figure 3 below.

The thing/device must authenticate itself, followed by the transfer of data to the cloud which is stored in a designated cloud database named "data sent by things/devices". The processing node embedded in the thing/device service manager also has to authenticate itself to gain access to the sent data by the authenticated devices. This data is then processed and stored in a database called "processed data for decision making". The receivers will need a subscription to this database in order to retrieve and issue an action command to the actuator.

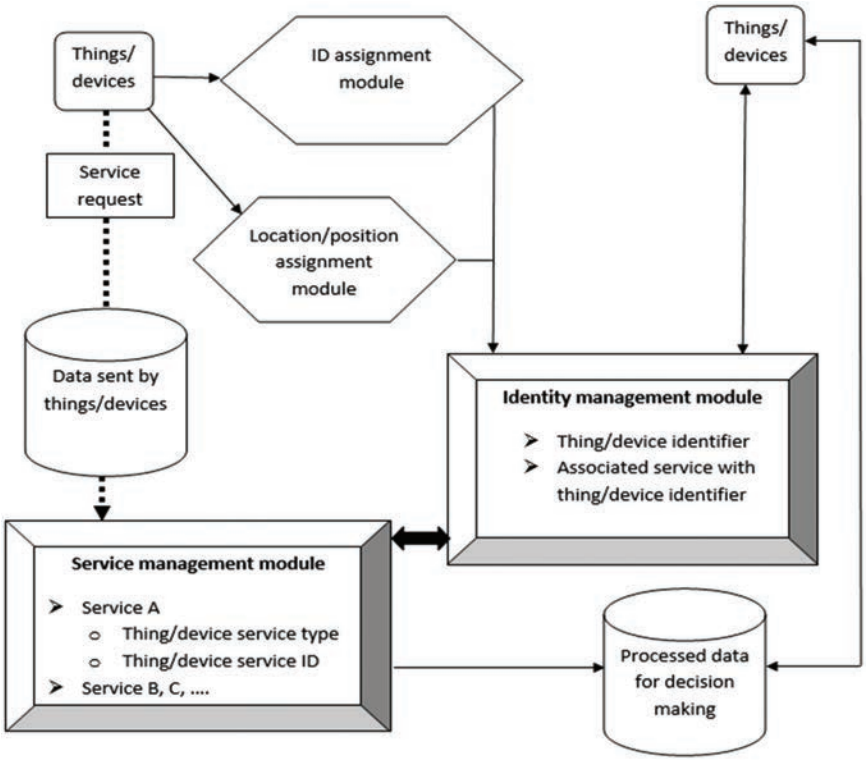

Figure 3 Identity management model for IoT.

In summary, the fundamental processes and functions of the identity management framework is to allow: enrollment of new things/devices into the IoT environment; things/devices and receivers enrollment to the cloud; identification of services sent to processing nodes by things/devices; authentication/authorisation of things/devices to execute service commands; removal of things/devices identity and services; and migration of things/devices to another networked platform. These are discussed in Table 4 below.

Table 4 Identity management framework scenarios, processes and functions for IoT

Scenarios	Process	Function (example)
Enrollment of new things/devices	When new things/devices are introduced to the IoT environment, a unique ID should be assigned to each thing/device by the identity manager, followed by notifications for authorisation of the new thing/device to access the environment but not any services.	New things/devices = {assign unique ID< thing/device service = null >}
Things/devices and receivers enrollment to the cloud	To be able to register things/devices and receivers to the cloud-IoT services, provision of a specific identification key/tag either by means of RFID, biometrics or QR codes is mandatory, as well as the position of these devices within the IoT environment must be known. This will enable the unique sign-up of each device to the cloud and allow an identity manager to distinguish data sent by each device.	Things/devices subscription = {thing/device ID< thing/device Type>, position ID}
Identification of services sent to processing nodes by things/devices	Since cloud-IoT services are expected to be categorised based on the type of things/devices data received and processed, therefore, each service must be uniquely assigned and identified by a service manager. The identity manager should also know the services and the things/devices subscribed to that service.	Service manager = {service Type = (for example: make coffee, wash dishes), <assign service ID>} Identity manager = {service ID <service Type>, things/devices subscription list}

(*Continued*)

Table 4 Continued

Scenarios	Process	Function (example)
Authentication and authorisation of things/devices to execute service commands	As soon as things/devices are authenticated and authorised to a particular cloud-IoT service, then they will be able to receive a signal for final execution of that service/task.	Things/devices authentication/authorisation = {<thing/device ID, service ID>, execution command = yes/no}
Removal of things/devices from service and identity manager database	For things/devices that wish to be removed or deregistered from the IoT environment and/or its associated cloud services, this change must be reflected/updated in the things/devices identity and service manager databases.	Removal of things/devices = { <delete thing/device ID, service ID>}
Migration of things/devices to another networked platform	When a thing/device is moved to another networked location within the same IoT environment, the position ID associated with that thing/device changes and therefore any associated services must be invalidated. For the thing/device to become active again, a new service that corresponds to its new location must be assigned.	Migration of things/devices = {<new position ID, thing/device ID>, <new service thing/device ID, service ID>}

Time-consumption of reviewing, managing, and uploading new identity and access modules that interface with existing and newly on-boarded IoT devices as well as updates should also be considered for the above framework. A cloud-IoT identity and access reliable model must considerably cut down processing (upload and download) time to suit immediate execution of commands/tasks [61]. Secure identity and access structure should be dependent on runtime environment that clarifies things/devices identity and interaction within the environment [62]. An identity and access intelligence console could further enable things or devices governance/control and visibility of their respective identities and access behaviour.

7 Conclusion

Internet of Things is an adaptive system with dynamic technical and physical attributes. This paper has reviewed and discussed the challenges for identity management in IoT. The requirements and management of things or devices

operating within an IoT environment have also been proposed using cloud as the base infrastructure for the management approach/model. This is due to the increasing reliance and shift of IoT's processing power to the cloud. Therefore, future work should be directed on the implementation of protocols for the proposed identity management model scenarios, processes and functions for IoT presented in this paper. Furthermore, new insights from innovations such as quantum computing are likely to make IoT even more compelling to society as the concept's results are geared towards revolutionising the way technology is adopted and applied in society.

References

[1] Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15), 2787–2805.

[2] Aijaz, A., and Aghvami, A. H. (2015). Cognitive machine-to-machine communications for Internet-of-Things: A protocol stack perspective. *IEEE Internet of Things Journal*, 2(2), 103–112.

[3] Holler, J., Boyle, D., Tsiatsis, V., Mulligan, C., and Karnouskos, S. (2014). *From Machine-to-machine to the Internet of Things: Introduction to a New Age of Intelligence*. Academic Press. 2.

[4] O'Neill, M. (2016). Insecurity by design: Today's IoT device security problem. *Engineering*, 2(1), 48–49.

[5] Lee, J. H., and Kim, H. (2017). Security and privacy challenges in the internet of things [security and privacy matters]. *IEEE Consumer Electronics Magazine*, 6(3), 134–136.

[6] Morgan, J. (2014). *A simple explanation of 'The Internet of Things'*. Available: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#415debcc1d09/

[7] Granjal, J., Monteiro, E., and Silva, J. S. (2010). Enabling network-layer security on IPv6 wireless sensor networks. In *2010 IEEE Global Telecommunications Conference (GLOBECOM 2010)*, 1–6. IEEE.

[8] Batool, K., and Niazi, M. A. (2017). Modeling the internet of things: a hybrid modeling approach using complex networks and agent-based models. *Complex Adaptive Systems Modeling*, 5(1), 4.

[9] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376.

[10] Lee, J. Y., Lin, W. C., and Huang, Y. H. (2014). A lightweight authentication protocol for internet of things. In *2014 International Symposium on Next-Generation Electronics (ISNE)*, 1–2. IEEE.

[11] Porambage, P., Schmitt, C., Kumar, P., Gurtov, A., and Ylianttila, M. (2014). Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. In *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, 2728–2733. IEEE.

[12] Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., and Wehrle, K. (2011). Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications*, 61(3), 527–542.

[13] Black, D., and McGrew, D. (2008). Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol (No. RFC 5282).

[14] Fremantle, P., Aziz, B., Kopecký, J., and Scott, P. (2014). Federated identity and access management for the internet of things. In *2014 International Workshop on Secure Internet of Things (SIoT)*, 10–17. IEEE.

[15] Ndibanje, B., Lee, H. J., and Lee, S. G. (2014). Security analysis and improvements of authentication and access control in the internet of things. *Sensors*, 14(8), 14786–14805.

[16] Aazam, M., Khan, I., Alsaffar, A. A., and Huh, E. N. (2014). Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved. In *2014 11th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 414–419. IEEE.

[17] Bandyopadhyay, D., and Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1), 49–69.

[18] Yan, Z., Zhang, P., and Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of network and computer applications*, 42, 120–134.

[19] Horrow, S., and Sardana, A. (2012). Identity management framework for cloud based internet of things. In *Proceedings of the First International Conference on Security of Internet of Things*, 200–203. ACM.

[20] Manyika, J. (2015). The Internet of Things: Mapping the value beyond the hype. McKinsey Global Institute.

[21] Farooq, M. U., Waseem, M., Khairi, A., and Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications*, 111(7).

[22] Lam, K. Y., and Chi, C. H. (2016). Identity in the Internet-of-Things (IoT): New challenges and opportunities. In *International Conference on Information and Communications Security*, 18–26. Springer, Cham.
[23] Friese, I., Heuer, J., and Kong, N. (2014) "Challenges from the Identities of Things: Introduction of the Identities of Things *discussion group within Kantara initiative*," in *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, 1–4: IEEE.
[24] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., and Kikiras, P. (2015). On the security and privacy of internet of things architectures and systems. In *2015 International Workshop on Secure Internet of Things (SIoT)*, 49–57). IEEE.
[25] Ashton, K. (2009). That 'internet of things' thing. *RFID journal*, 22(7), 97–114.
[26] Kolias, C., Kambourakis, G., Stavrou, A., and Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80–84.
[27] Gudymenko, I., Borcea-Pfitzmann, K., and Tietze, K. (2011). Privacy implications of the internet of things. In *International Joint Conference on Ambient Intelligence*, 280–286. Springer, Berlin, Heidelberg.
[28] Dimov, D. (2013). Privacy Implications of the Internet of Things. *InfoSec Institute*, 14.
[29] Botta, A., De Donato, W., Persico, V., and Pescape, A. (2016). Integration of cloud computing and internet of things: a survey. *Future Generation Computer Systems*, 56, 684–700.
[30] Jiang, L., Da Xu, L., Cai, H., Jiang, Z., Bu, F., and Xu, B. (2014). An IoT-oriented data storage framework in cloud computing platform. *IEEE Transactions on Industrial Informatics*, 10(2), 1443–1451.
[31] Li, F., Vögler, M., Claeßens, M., and Dustdar, S. (2013). Efficient and scalable IoT service delivery on cloud. In *IEEE Sixth International Conference on Cloud Computing (CLOUD)*, 740–747. IEEE.
[32] Moosavi, S. R., et al. (2015). SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Computer Science*, 52, 452–459.
[33] Ren, W., Yu, L., Ma, L., and Ren, Y. (2013). How to authenticate a device? Formal authentication models for M2M communications defending against ghost compromising attack. *International Journal of Distributed Sensor Networks*, 9(2), 679450.
[34] Xue, K., Ma, C., Hong, P., and Ding, R. (2013). A temporal-credential-based mutual authentication and key agreement scheme for wireless

sensor networks. *Journal of Network and Computer Applications,* 36(1), 316–323.

[35] Hayashi, E., Das, S., Amini, S., Hong, J., and Oakley, I. (2013). CASA: context-aware scalable authentication. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, 3. ACM.

[36] Kayacik, H. G., Just, M., Baillie, L., Aspinall, D., and Micallef, N. (2014). Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors. *arXiv preprint arXiv:1410.7743*.

[37] Shi, E., Niu, Y., Jakobsson, M., and Chow, R. (2010). Implicit authentication through learning user behavior. In *International Conference on Information Security,* 99–113. Springer, Berlin, Heidelberg.

[38] Chun, S., Jung, J., Jin, X., Cho, G., and Lee, K. H. (2014). Semantically enriched object identification for Internet of Things. In *2014 IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 141–142. IEEE.

[39] Ning, H., and Wang, Z. (2011). Future internet of things architecture: like mankind neural system or social organization framework? *IEEE Communications Letters,* 15(4), 461–463.

[40] Singhanat, K., Harris, N. R., and Merrett, G. V. (2016). Experimental validation of opportunistic direct interconnection between different Wireless Sensor Networks. In *2016 IEEE Sensors Applications Symposium (SAS)*, 1–6. IEEE.

[41] Ding, D., Li, M., and Zhu, Z. (2018). Object Naming Service Supporting Heterogeneous Object Code Identification for IoT System. In *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, 545–554. IEEE.

[42] Zhang, H., and Zhu, L. (2011). Internet of Things: Key technology, architecture and challenging problems. In *2011 IEEE International Conference on Computer Science and Automation Engineering (CSAE),* 4, 507–512. IEEE.

[43] Khoo, B. (2011). RFID as an Enabler of the Internet of Things: Issues of Security and Privacy. In *Internet of Things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing*, 709–712. IEEE.

[44] Liu, C. H., Yang, B., and Liu, T. (2014). Efficient naming, addressing and profile services in Internet-of-Things sensory environments. *Ad Hoc Networks*, 18, 85–101.

[45] Roman, R., Najera, P., and Lopez, J. (2011). Securing the internet of things. *Computer,* 44(9), 51–58.

[46] López, T. S., Brintrup, A., Isenberg, M. A., and Mansfeld, J. (2011). Resource management in the Internet of Things: Clustering, synchronisation and software agents. In *Architecting the Internet of Things*, 159–193. Springer, Berlin, Heidelberg.

[47] Hong, S., Kim, D., Ha, M., Bae, S., Park, S. J., Jung, W., and Kim, J. E. (2010). SNAIL: an IP-based wireless sensor network approach to the internet of things. *IEEE Wireless Communications*, 17(6).

[48] Lee, J. J., Hong, Y. S., and Lee, K. Y. (2015). An authentication scheme based on elliptic curve cryptosystem and openID in the internet of things. In *Proceedings of the International Conference on Security and Management (SAM)*, 192. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[49] Mahalle, P. N., and Railkar, P. N. (2015). *Identity management for internet of things*, 39. River Publishers.

[50] Beltran, M. (2018). Identifying, authenticating and authorizing smart objects and end users to cloud services in Internet of Things. *Computers & Security*.

[51] Kamath, S. H., Pandey, S., and Tanisha, K. (2017). Security Issues in Internet of Things. *International Journal of Emerging Research in Management & Technology*, 6(5), 260–264.

[52] Dihal, S., Bouwman, H., de Reuver, M., Warnier, M., and Carlsson, C. (2013). Mobile cloud computing: state of the art and outlook. *info*, 15(1), 4–16.

[53] Fazio, M., Celesti, A., Villari, M., and Puliafito, A. (2014). The need of a hybrid storage approach for iot in paas cloud federation. In *2014 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 779–784. IEEE.

[54] Walraven, S., Truyen, E., and Joosen, W. (2011). A middleware layer for flexible and cost-efficient multi-tenant applications. In *ACM/IFIP/USENIX International Conference on Distributed Systems Platforms and Open Distributed Processing*, 370–389. Springer, Berlin, Heidelberg.

[55] Chen, S. L., Chen, Y. Y., and Hsu, C. (2014). A new approach to integrate internet-of-things and software-as-a-service model for logistic systems: A case study. *Sensors*, 14(4), 6144–6164.

[56] Butzin, B., Konieczek, B., Golatowski, F., Timmermann, D., and Fiehe, C. (2016). Applying the BaaS reference architecture on different classes

of devices. In *2016 2nd International Workshop on Modelling, Analysis, and Control of Complex CPS (CPS Data)*, 1–6. IEEE.

[57] Khajeh-Hosseini, A., Greenwood, D., and Sommerville, I. (2010). Cloud migration: A case study of migrating an enterprise it system to iaas. In *2010 IEEE 3rd International Conference on Cloud Computing (CLOUD)*, 450–457. IEEE.

[58] Limoncelli, T., Chalup, S. R., and Hogan, C. J. (2014). The Practice of Cloud System Administration: *Designing and Operating Large Distributed Systems*, 2. Pearson Education.

[59] Chen, D., and Zhao, H. (2012). Data security and privacy protection issues in cloud computing. In *2012 International Conference on Computer Science and Electronics Engineering (ICCSEE)*, 1, 647–651. IEEE.

[60] Ferreira, J. A. L., and da Silva, A. R. (2014). Mobile cloud computing. *Open Journal of Mobile Computing and Cloud Computing*, 1(2), 59–77.

[61] Celesti, A., Tusa, F., Villari, M., and Puliafito, A. (2010). Security and cloud computing: Intercloud identity management infrastructure. In *2010 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE)*, 263–265. IEEE.

[62] Naik, N., and Jenkins, P. (2016). A secure mobile cloud identity: Criteria for effective identity and access management standards. In *2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 89–90. IEEE.

Biographies

Abubakar Bello received his doctorate in IT with a technical, business and social focus on Cyber Security and Privacy, MBA with specialisation in ICT, and MSc and BSc (Software Engineering) in Computer Science. Dr. Abubakar has extensive research and teaching experience across information systems security management, and also worked across several corporations, privately held entities and government organisations where he provided security and privacy audit and risk management services. He also has a strong expertise in behavioural security analysis and continues to play a key role in security design innovation.

Venkatesh Mahadevan gained his Bachelor's and Master's in Engineering, and Doctorate in Management Information Systems. Associate Professor Venkatesh has extensive teaching and research experience around the security of information systems, including many expert evaluations of different business management systems (such as Patient Management Information System, Hotel Management Information System and Remotely Accessible Management Information System for Vehicle Inspectors). Also, he has strong expertise in the end-to-end delivery of customer centric technology innovation and continues to play a major role in the planning and development of several IT management security-centric solutions.