



Data trust in Consumer Internet of Things assemblages in the mobile and fixed telecommunication operators in South Africa

**Authors:**

Mfanasibili Ngwenya¹ 
Mpho Ngoepe¹ 

Affiliations:

¹Department of Information Science, Faculty of Human Sciences, University of South Africa, Pretoria, South Africa

Corresponding author:

Mfanasibili Ngwenya,
mfanasibili@hotmail.com

Dates:

Received: 16 June 2021

Accepted: 27 Jan. 2022

Published: 28 Mar. 2022

How to cite this article:

Ngwenya, M. & Ngoepe, M., 2022, 'Data trust in Consumer Internet of Things assemblages in the mobile and fixed telecommunication operators in South Africa', *South African Journal of Information Management* 24(1), a1426. <https://doi.org/10.4102/sajim.v24i1.1426>

Copyright:

© 2022. The Authors.
Licensee: AOSIS. This work is licensed under the Creative Commons Attribution License.

Background: Devices can be connected through the Internet of Things (IoT) technology to create a smart ecosystem. From the connection, various stakeholders share personal data with companies in the consumer IoT (CIoT) space for marketing and other reasons. Customers download and use applications without mulling over the type of personal information exposed to the rest of the world.

Objective: The main objective of this study was to explore data trust in CIoT assemblages in the mobile and fixed telecommunication operators in South Africa.

Method: This qualitative study triangulated narrative enquiry with the Delphi technique to explore data trust in CIoT assemblages in South Africa. The primary data collection techniques used in this study were unstructured interviews (in the case of narrative enquiry), questionnaires and semi-structured interviews (in the Delphi technique). For the Delphi technique, five experts were chosen purposively based on their involvement in IoT, selling and on-selling IoT services or those providing support services to the IoT ecosystems, while six narrative enquiry participants were selected through snowball technique based on their exposure to using consumer IoT solutions, ability to provide detailed descriptions of their experiences and willingness to articulate those experiences.

Results: The study established that the choice of system to use varied from consumer to consumer. The consumer's original decision may be influenced by many factors, such as devices sponsored by one's health insurance or security company. However, the constant use of a specific system makes it personal and more comfortable for the consumer. The level of trust in the CIoT system increases with constant interactions.

Conclusion: The study concludes that there should be a very high level of stakeholders trust for faster adoption of CIoT in South Africa. Therefore, regulators such as the Independent Communication Authority of South Africa should ensure that IoT devices in the South African market are trustworthy.

Keywords: data trust; data security; Consumer Internet of Things (CIoT); mobile applications; South Africa.

Introduction

Many types of technologies such as big data, the internet of things (IoT) and artificial intelligence expose people's private lives in one way or another. For example, DeLanda (2016) argued that IoT technology allows people to connect all their devices and create a smart ecosystem or what he calls an assemblage, thus making a person's life a far more integrated one. Each of these devices has internet connections allowing sharing of personal data with the mobile application (mobile app) developers and their partners or any other stakeholders. As Ngwenya and Ngoepe (2020) pointed out, 'it is important for consumers to be aware of new technologies' benefits and risks.' Consumers judge the quality of smart home systems based on the functioning of the IoT mobile app.

The rise of the IoT has driven mobile apps development. According to Schmitt et al. (2018), IoT connects various devices via the internet with various resources such as 'memory, computational capacity and energy consumption.' For example, in the consumer IoT (CIoT) space, any product almost always comes with a smartphone application to either control, programme or just view what is happening with the product. Tiwary et al. (2018) pointed out that the consumer has to download the required application using a smartphone, a tablet or a laptop. This application can communicate with a centralised database and obtain valuable data about the environment.

Read online:

Scan this QR code with your smart phone or mobile device to read online.

Consumer internet of things improve efficiency, analytics, intelligence and decision-making. These beneficial attributes of CIoT are achievable only if the data collected are trustworthy. Ayaz (2019) highlighted that a 'trustworthy digital system should preserve its users' privacy' as this is one way to gain consumer trust.

Ngoepe and Ngwenya (2022) alluded that consumers often overlook the security risks of smart devices. Fong, Lam and Law (2017) stated that consumers more often than not download and use applications without having a second thought regarding the information they may indirectly be sharing with the rest of the world. Smart devices collect data and track consumers' behaviour. However, some consumers are not aware of the activities of their smart devices, such as data collection, tracking and even where the storage of their data is. As a result, the trust of CIoT comes into question. This study focused on data trust as far as it relates to storage, connectivity, management and processing issues. The following questions relating to CIoT come to mind while using mobile apps and interacting with smart devices:

- Who can have access to the collected data?
- Where do service providers store the data that they collect?
- Who owns the data that service providers collect?
- What do service providers do with the data they collect?

The data in question may reside anywhere in the world. Each country has its own set of laws concerning data privacy and ownership. Regardless of where the data reside in the world, the trust issues are real, and the internet has no boundaries. The connection of different gadgets via the internet using memory, energy consumption and computational ability has raised data trust issues in IoT. Duranti (2020) observed that the 'trust level is proportional to the data's sensitivity, the vulnerability of its environment and the adverse consequences or loss of trustworthiness.'

Problem statement

Internet-of-things devices generate a massive amount of data. Such data can be used to benefit humankind, save lives, convict criminals and curb further criminal activities. However, the same data can be used for nefarious means by criminals. Criminals may use data from IoT assemblage to steal personal information that includes financial information or one's identity. Rose, Eldridge and Chapin (2015) acknowledge that there has always been a concern in information technology when it comes to security. Palattella et al. (2016) acknowledged that fitness and health tracking systems, smartwatches and sensor-rich smartphones may expose sensitive data such as someone's health status or life habits.

Ali et al. (2018) asserted that consumers of IoT do not have total confidence and control over how service providers use the data they share and, therefore, do not trust the CIoT ecosystem. Moreover, Rose et al. (2015) alluded that when IoT devices connect to the internet without proper security by the CIoT service providers, they compromise the safety of

the consumers and the resilience of the internet. This threat is further made worse by:

- the massive deployment of these heterogeneous CIoT devices
- devices being able to link to other devices automatically
- deploying the devices, environments that are not safe.

The emerging literature on consumer-object interaction identified trust concerns as being amongst the critical hindrances of the widespread adoption of CIoT (Babar et al. 2010; Lee & Lee 2015). When service providers do not attend to these trust concerns, the results may be reduced adoption by consumers. Ali et al. (2018) mentioned that gathered data from CIoT devices may have private and confidential information, which means it is essential for consumers to trust the safety of their personal information.

Literature review

Trust comes in many different forms. Chen, Bao and Guo (2015) alluded to social trust metrics such as honesty, cooperativeness and community interest. These trust metrics complement each other. Diamantopoulou et al. (2020) stated that some consumers are complacent with their personal information and express implicit trust in their service providers and governments, believing that they will protect them from the unlawful use of their data.

Ngwenya and Ngoepe (2020) asserted that 'consumers need to be comfortable in sharing personal information with other stakeholders in a CIoT assemblage'. Indeed, the exchange of information is essential for CIoT to succeed. In the exchange of information, sensitive data should be protected. According to Ngwenya and Ngoepe (2020), trust 'should be incorporated and built into the system at the design stage of CIoT systems'.

This will lead to a trustworthy relationship between stakeholders in the CIoT systems. The stakeholders include 'cloud providers, device manufacturers, connectivity providers and mobile app developers', to mention just a few (Gao & Bai 2014).

Trust is about a person's perceptions of another person's integrity and ability or another service system (Cheng et al. 2019). When Tchernykh et al. (2016) discussed trust, they emphasised that unauthorised people can alter the data. It is hard to argue whether a system is trustworthy because there are no existing metrics to measure this. A matrix is valuable and developers, integrators and regulators, amongst other stakeholders can use it. Chen et al. (2015) stated the three trust metrics: honesty, cooperativeness and community interest. For example, malicious code represents dishonesty and is dangerous to the consumers and other elements of an IoT assemblage. Such a code can severely disrupt the operations of the whole system and thus service continuity. Laplante and Applebaum (2019) stated that when trust in the system is broken, other things such as data integrity are affected. The integrity of data is essential and is directly

related to trust. Data integrity is about the quality of the data generated by or fed into an IoT system.

There is continuous interaction in any CIoT assemblage, and each element or stakeholder relies on others. Chen et al. (2015) stated that the willingness or ability of objects and stakeholders to cooperate represents the level of trustworthiness. Yan, Zhang and Vasilakos (2014) stated that trust is about a declaration of holistic credential information or disclosure of relevant information, often decentralised across a network of actors and objects. Ayaz (2019) ascertained a healthy relationship between trust and security because ensuring system security and consumer safety is necessary to gain confidence. In addition, a strong relationship exists between trust and privacy as it touches on the strength of an object to determine the release and disclosure of information. Ngwenya and Ngoepe (2020) stated that trust may be compromised at many levels, namely 'consumer level, device level and network level'.

Consumer level

Ngwenya and Ngoepe (2020) asserted that consumers take trust issues seriously as companies or individuals manipulate the data for some nefarious gains. For instance, some consumers use fitness monitoring equipment to accumulate points by putting these devices on dogs or cats. According to Ngwenya (2020), 'the purpose of having these wearables is to ensure that people remain active for health purposes.' However, as observed by Ngwenya and Ngoepe (2020), 'the collected data are incorrect, as the active entity is a dog or cat.' In South Africa, companies such as Discovery, through their Vitality Health programme, have struggled with trust for a long time because it is not easy to tell if the entity exercising is a person, a dog or another entity. This example clearly shows that the collected data lacks credibility as the device was used for the wrong purpose. Organisations should ensure that the data collected from consumers and devices are trustworthy. Then the question by Ngwenya and Ngoepe (2020) on 'what precautions can organisations take to safeguard and trust the accuracy of the data from consumers?' is relevant to ask.

Consumer trust in CIoT grows based on the reliability of the system. For example, if a person leaves home forgetting to switch off the stove or geyser and controls anything remotely, the CIoT assemblage needs to help the consumer at all times. If the system reports that the person has successfully turned off the stove, it has to be like that. That is how trust is built – the system has to be reliable. However, the trust is broken if the consumer comes home and discovers that the system did not switch off the stove per expectation. This broken trust is between the CIoT system and the consumer. Sometimes, trust can be broken between a specific device and the CIoT system or just between a device and the consumer. For the consumer to trust a system, that system has to be reliable at all times. There may be a need for reliability assessments of the system. Can the system handle anomalous events and data?

Usability is critical from a consumer perspective. Laplante and Applebaum (2019) stated that 'usability is a trust concern that deals with whether consumers understand how to use the devices they can access'. The question is about the user-friendliness of the IoT devices, mobile apps or other display modes and the ability to learn how to use the overall system. Laplante and Applebaum (2019) further stated that the 'user interface does not need to be constrained by limited display size and functionality'. The authors argue that usability has implications on user trust.

Smart devices level

All stakeholders interested in the collected data need to trust the devices that collect the data. If the equipment is faulty and collects untrustworthy data, the consequences can be dire and even life threatening (Ngwenya & Ngoepe 2020). Default credentials are still widely used and this exacerbates the issue of trust. Criminals may counterfeit IoT devices. Trust has to exist from data collection up to the stage of data storage. Ouaddah, Abou Elkalam and Ait Ouahman (2016) mentioned that those interacting devices that make up IoT reside at the edges.

Internet-of-things data generation and action thereof happens at the edges. As observed by Ouaddah et al. (2016), 'there are often no secure physical perimeters where the physical world's raw sensing takes place', such as on rooftops and geysers, in our gardens, inside our car engines and on solar panels. The threats to IoT devices are an essential concern because they are hard to remediate and fix.

Third-party devices also come with trust issues. More often than not, we do not know what is happening inside third-party devices. Laplante and Applebaum (2019) stated that ownership and control are trust concerns when much of the IoT system's functionality originates from third-party vendors. If we do not know the internal workings of a third-party device, it can lead to security threats from the device in question. These devices are neither observable nor transparent and can contain malicious Trojan behaviours. Consumers of IoT can only hope and trust that there is no malicious intent by third-party providers. Laplante and Applebaum (2019) argued that when CIoT adopters start understanding the magnitude of losing access to these acquired functions, they will recognise the criticalness of IoT systems' trust. Palattella et al. (2016) stated that the increase in the number of devices and the exchange of data multiplies the systems' vulnerabilities, thus becoming more susceptible to privacy leaks and attacks from the internet.

There is also a trust concern between hardware and software components. Will they always work well with each other? Interoperability can be a challenge in a system with heterogeneous devices. The devices or device parts should be swappable to satisfy new system requirements. After that, these devices should continue communicating without breaking the trust that existed before swapping a specific device or component. That means trust relates to integration, interoperability, compatibility and composability. Each of

these has an impact on IoT trust. It may help to evaluate the properties of new devices or components of a device entering the system before being part of the assemblage.

Network and storage level

Network-level trust refers to end-to-end communication between smart things and consumers. Ngwenya and Ngoepe (2020) came up with a series of questions to explore trust issues at the network and storage level as follows:

- What are the threats to these networks?
- How can a communication path in these networks be secured?
- Can the network be trusted not to compromise data or allow data alteration and misinform consumers or stakeholders interested in the collected data?
- Do consumers always know what smart devices are doing?
- If we consider a voice response technology such as smart speakers, Amazon Alexa and Google Assistant, do consumers know who else might be listening?
- Are these sounds stored somewhere and linked to the consumer?

The network helps to synchronise the CIoT system, especially as far as redundancy and backup are concerned.

According to Laplante and Applebaum (2019), these systems have 'several computations, events and functions, such as data transfers, happening simultaneously'. Chen et al. (2011) suggested that the data exchange happens throughout the ecosystem, and unauthorised access exposes it to data theft, the supply of fake data and viruses. They further mentioned that data related to destination and source at the network layer level are easy to alter and thus compromise the privacy of consumers of IoT. It is, indeed, essential to use access control management at the application level. As mobile apps operate at the application level, developers of mobile apps have to do due diligence during the development process as far as access control management is concerned. However, as the mobile apps are just an element of a broader IoT ecosystem, other layers of the IoT ecosystem may be used as entry points of attack, which renders access control management at the application level lacking in security.

Sivarajah et al. (2017) stated that IoT results from sensors and machines working together. The IoT value comes when sensors gather data and leverage it. Sadeghi, Wachsmann and Waidner (2015) argued that 'cloud-based applications are the key to leveraging data'. Want, Schilit and Jenson (2015) agreed and stated that 'the cloud enables the apps to work for you anytime, anywhere'. Mollah, Azad and Vasilakos (2017) observed that to 'protect data confidentiality and privacy, there is a need to ensure mobile device storage security'. Tiwary et al. (2018) agreed with the latter approach and proposed centralised architectures. Ali et al. (2018) argued that centralised cloud services have made significant contributions to IoT growth. However, they admit that a centralised approach can hinder the development of the IoT because of the potential risks

associated with a single point of failure when the system is under attack. When the cloud services such as the database are centralised and are under lethal security attack or have faults, the attacker may bring down the whole assemblage. However, a centralised approach introduces a single point of failure, and personal data may be compromised even more in this architecture. Ensuring that information is trustworthy is difficult enough when a central authority orchestrates device configuration, data collection and cleaning, and data dissemination. However, distributed networks such as those using blockchain technology do not rely upon a central authority.

Some scholars (Hashemi et al. 2016; Pilkington 2016) proposed a blockchain architecture in dealing with trust issues from a network architecture perspective to eliminate the single point of failure. However, in reality, trust extends beyond the devices part of a blockchain. Crosby et al. (2016) defined blockchain as a 'distributed database of records' or a public ledger of all transactions or digital events that have been 'executed and shared by participating parties'. According to Zyskind and Nathan (2015), 'distributed ledger technologies come with promises of shared trust in information created and exchanged by smart things and people'. Biswas and Muthukkumarasamy (2016) agreed and stated that the main benefits of using blockchain are its resiliency against many threats, improved reliability, better fault tolerance capability, 'faster and more efficient operation and scalability'.

Research methodology

This qualitative study triangulated narrative enquiry with the Delphi technique to explore data trust in CIoT assemblages and associated mobile applications in South Africa. The primary data collection techniques used in this study were unstructured interviews, participant observation (in the case of narrative enquiry), questionnaires and semi-structured interviews (in the Delphi technique). The data collection was in two parts.

The first part used the narrative enquiry method, whereby the format was in unstructured interviews. The second part used the Delphi technique, whereby experts' opinions were sorted using structured and semi-structured interviews. The researcher allowed the participants to express themselves beyond any predefined question in both cases. The chosen experts would have been involved in IoT, selling and on-selling IoT services or those providing support services to the IoT ecosystems. This sample was from the mobile and fixed services operators in South Africa such as Vodacom, Telkom, MTN and Liquid Telecoms. The participants' identities remained confidential throughout the research process. The researchers named participants as 'participant, followed by a letter and number' to ensure anonymity, as follows:

- the naming of participants from narrative interviews: Participant A1 through to A6
- the naming of participants from Delphi approach interviews: Participants B1 through to B5.

Narrative enquiry

According to Creswell and Poth (2017), narrative enquiry is 'open-ended, seeking to understand participants' experiences rather than seeking measurable and observable data where the research questions are specific and narrow'. People are storytellers by nature, and they find meaning from the stories they tell. The narrative enquiry allows people to tell their experience from consuming IoT services in this study. Different consumers have different experiences, so are the stories they tell. Clandinin (2006) stated that narrative enquiry is about narrating lived experiences. As consumers interact with things in an IoT ecosystem, we can understand their lived experiences through storytelling or narrative enquiry. However, the 'experiences and stories bring a new coherent narrative that makes sense to us' (Ngoepe & Ngwenya 2022). The new coherent narrative influences consumers' future decision making. In the case of trust issues regarding the IoT ecosystem, if consumers trust the IoT services, they are more likely to buy or recommend them to other consumers. The reverse is equally true if consumers feel like they cannot trust the ecosystem.

The researchers interviewed and recorded six participants, lasting for about 30 min each. The full recordings across the participants was 187 min. The researchers selected the participants based on snowball techniques on their exposure to using consumer IoT solutions, ability to provide detailed descriptions of their experiences and willingness to articulate those experiences. The researchers were tactful when asking questions to get the most out of the interviews. The idea is that the researchers should not unnecessarily interject, direct the conversation or limit the participant from telling their lived experiences. Scârneci-Domnişoru (2013) stated that the narrative enquiry allows researchers to approach research topics with less detailed guides and without predefined-answer surveys, thus allowing the participants to have greater freedom to express themselves. The researchers transcribed the data from recorded interviews before analysing it. Transcribing helped the researchers understand the interviews in detail and enabled ideas to flow, thus making it easier to interpret the text.

Delphi technique

The Delphi technique aimed to seek experts' opinions or knowledge to understand a phenomenon under study in greater depth within their domain of study. The researchers considered participants as experts based on their field of work as it related to IoT and the number of years working in that field. The researchers sought out permission before sending the surveys to the participants. According to Bryman (2016), the Delphi technique explores the underlying assumptions or information, leading to different judgements. The process is such that the information obtained may generate consensus amongst the experts. The researcher used three iterations before reaching a consensus from the experts. This research study's primary data collection techniques were semi-structured interviews and questionnaires. The experts' opinions sought to explain the trust issues in an IoT assemblage and highlight practical approaches. Skulmoski,

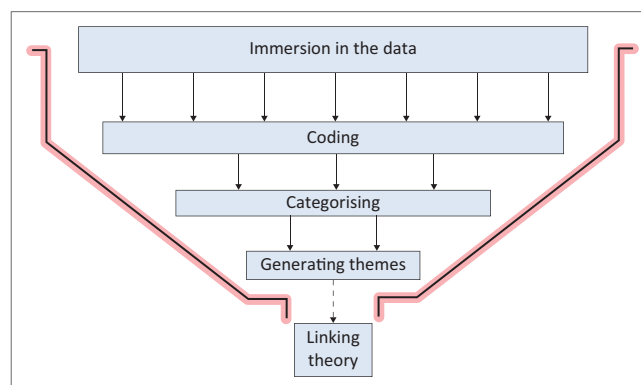
Hartman and Krahn (2007) stated that Delphi technique is suitable for capturing rigorously qualitative data. The researchers acknowledge that the IoT industry is a specialised field within the information and communication technology (ICT) industry. Thus, experts' opinions were an essential critical input to the study dealing with IoT trust issues.

Data presentation and analysis

The researchers used thematic analysis to analyse data collected from both narrative enquiry and Delphi technique. The narrative enquiry method involves the identification and reporting of patterns called themes. The researcher retrieved these themes from the primary qualitative data. The researcher utilised the technique to classify and organise data according to key themes, concepts and categories. Jovchelovitch and Bauer (2000) mentioned that as the narrative interview is a technique for generating stories, it is open concerning the analytical procedures that follow data collection.

In the Delphi technique, the thematic analysis was iterative while collecting the data. There were three rounds of questionnaires sent to the experts via email. Braun and Clarke (2006) stated that thematic analysis is a method rather than a methodology. Therefore, it is not tied to a particular epistemological or theoretical perspective, thus making it very flexible. The researchers used thematic analysis in the data collected using the Delphi Technique. The Delphi method can employ various analytical techniques depending on the research purpose and collected data. The researchers developed questions from the previous round of the Delphi technique by thematic analysis. Whenever a researcher uses the Delphi technique, he conducts the analysis iteratively throughout the study, as prior waves of data collection must be analysed to inform the questionnaires developed for subsequent waves of the survey. Figure 1 summarises the steps involved in the analysis of qualitative data.

The presentation and analysis of collected data began by transcribing audio interviews, reading the interview transcripts and finally, reading the answers from the



Source: Braun, V. & Clarke, V., 2020, 'One size fits all? What counts as quality practice in (reflexive) thematic analysis?', *Qualitative Research in Psychology* 18(3), 328–352. <https://doi.org/10.1080/14780887.2020.1769238>; Kiger, M.E. & Varpio, L., 2020, 'Thematic analysis of qualitative data: AMEE Guide No. 131', *Medical Teacher* 42(8), 846–854. <https://doi.org/10.1080/0142159X.2020.1755030>; Liebenberg, L., Jamal, A. & Ikeda, J., 2020, 'Extending youth voices in a participatory thematic analysis approach', *International Journal of Qualitative Methods* 19, 1609406920934614. <https://doi.org/10.1177/1609406920934614>

FIGURE 1: Steps in qualitative data analysis using thematic analysis.

questionnaires. The latter part happened iteratively throughout the process. After that, the researchers worked on the coding process and categorisation of the collected data. The next stage of the analysis generated themes from codes and categories. The authors generated themes from both narrative enquiry data and Delphi technique data. From the categories grouped, the researchers generated the following central themes: trust issues, transparency by cloud providers, app developers and device manufacturers, enforcement by regulators and stakeholders using personal data for nefarious purposes.

Data trust in consumer Internet of Things

Participants A1, A2, A3 and A5 mentioned that they trust the internal policies already implemented by original equipment manufacturers (OEMs) of either IoT devices or the apps used to control those devices. Participants A4 and A6 believed that trusting the global brands that provide CIoT in one way or the other is equivalent to being naïve, and the onus should always be with the consumers to protect themselves. The experts (Participants B1 to B5) agreed that all stakeholders in the CIoT assemblage should be responsible for enforcing trust.

Participant A3 felt that he is co-creating the future technology by allowing OEMs to use his data and personal information. He stated that:

'I feel like I am part of the creation of new technologies and innovations. I do not believe I should be paying for the devices. The providers should incentivise us for allowing them to use our data. These companies use our data to innovate and provide better services in future, and hence I feel I am responsible for contributing to innovation. I am happy to pay for the extra value-added services but not the hardware.'

Participant A2 voiced that:

'Consumers, as part of the stakeholders, may use the devices in an untrustworthy way. I have in mind the Discovery Health app that rewards physically active consumers. Some people put the wearables on dogs and accumulate many steps in a day and thus gain points that help reduce the premium or get other rewards. Putting the wearables on the dogs defeats the purpose of rewarding active members. This has greatly compromised trust between the service provider (Discovery Health) and the member or consumer.'

The underlying contract is that the consumer gives up a little privacy and receives valuable information. Participant A2 further ascertained that:

'Like most people, I value my data. When I use an IoT provider's site or device, there exists a psychological contract that the provider can use my information. The terms and conditions of most, if not all, providers state that they can use my data for various purposes, including research purposes, marketing and sharing with their partners. I trust that the service providers will safeguard my information and are not going to use my information to damage my reputation.'

Almost all health apps are free. However, Participant A2 mentioned that:

'Free is not necessarily free. Companies will always find a way of monetising your data. For example, Discovery Insure track drivers' behaviour with the promise of lowering the premiums if they prove to be good drivers. However, the company might use your information to build a case for future claims so that they can reject those future claims.'

Participant A4 uses the Mercedes me connect apps to interact with his car. He suggested that:

'As far as I am concerned, the technology of connected cars can go a long way in curbing crime in South Africa. Historically, people depended a lot on Tracker to locate stolen vehicles or investigate crimes committed. Over the years, Tracker has been working very closely with insurance companies, and those insurance companies have increasingly declined claims based on the data they get from Tracker.'

However, most participants agreed that there is a need for service providers to be transparent in detailing how they will use the consumers' data. Stakeholder trust looks at how different stakeholders use personal identifiable information (PII) and how that information benefits the consumer. At what cost is personal information used, and can the end consumer trust that service providers or any stakeholders positively use their data? Participant A2 voiced out his trust on established brands by stating that:

'I trust global brands such as Apple or Samsung and believe they cannot use or share my information for malicious use.'

Participant A2's response shows that stakeholder trust can be related to the branding of those stakeholders. The participants addressed stakeholder trust as a way of trusting private companies in the form of OEMs, app developers or cloud providers to keep their data secure. Companies would typically use the collected data to understand better and service their customers and upsell new services in future. Most participants did not welcome the idea of companies tracking them. Participants A1, A3, A4 and A5 felt that companies collect too much personal data. Participant A2 believed that data collection, especially by trusted brands, is a good thing as they can use that data to advance new technological innovation and service their customers better. He had a view that he was part of co-creation.

Participant A4 felt comfortable having the location-based information shared with Mercedes. He mentioned that this could be for his protection when something wrong happens. However, he warned against using a similar technology with insurance companies. He felt insurance companies, especially in South Africa, are untrustworthy.

Some participants were not aware of where their personal information resided. Some participants stated that their data lived in the cloud. Others held the view that their data lived in their phones or any of the devices they were controlling. None of the participants were confident enough to state with certainty where their data resided. Furthermore, the participants struggled to say confidently how CIoT service providers were using their data. However, participant A2's trust in big corporates was visible as he stated that:

'The benefits are much higher than the risks, and these are global companies with advanced internal policies that respect people's privacy. Maybe I am naïve, but I feel I am helping them to create better services in the future.'

The view of experts (Participants B1 to B5) from the Delphi technique was that lawmakers are always behind when it comes to technological advancements. They agreed that South Africa has not been focusing on regulating IoT technology. For example, Participant B2 commented that:

'Technology is evolving too fast for lawmakers to understand what is happening.'

They further agreed that if South Africa does not address privacy and security issues, the national security information, business secrets and personal privacy may be compromised and detrimental to its development. Therefore, South Africa needs a legal point of view to promote the development of the IoT. Participant B5 stated that:

'There is a dire need for policies and regulations, and there is still much work to do in that area.'

Discussions

The level of trust is of the utmost importance through the CIoT assemblage and between all stakeholders. For example, consumers interact with their smart things, such as the smart home, until they trust it to operate as it should. The constant interactions create a true dependency. Communications amongst all of the components matter in assemblage theory. The interactions amongst the components that do not involve the consumer also contribute to indispensability and other outcomes.

The relationships between consumers and smart devices are personal. The interactions with the machines are personal and diverse from one consumer to another. For example, the study's findings showed that the choice of system to use for either home security purposes or personal fitness purposes varied from one consumer to another. The consumer's original decision may be influenced by factors such as devices sponsored by one's health insurance (as in the case with the participant who uses Discovery Medical Aid). However, the constant use of a specific system makes it personal and more comfortable for the consumer. The level of trust in the provider and the CIoT system they provide increases with the constant interactions.

The researcher's wishes are that insurance companies do not use personal information as a tool to decline claims in the future. In the case of car insurance, they may use driving behaviour to reject claims. While the current researchers agree that people should be responsible drivers, car insurance drivers should issue warnings to their clients about their driving habits. They further need to state the consequences of continued bad driving habits. Such behaviour could result in the cancellation of the consumer's membership if need be. The problem is when the insurance company collects the clients' premium while being aware of its risky behaviour.

The consumers saw the benefits of automating some routine tasks using CIoT. The CIoT does everyday tasks as if the consumer himself or herself is doing them. The assemblage theory makes us understand the importance of all the component interactions and stakeholders. The question arises as to whether automating mundane tasks will make the South African society more productive in the long term.

Conclusion and recommendations

This study revealed that the development of the CIoT brings with it trust issues. The study showed that trust happens at the consumer, smart devices, and network and storage levels. Each level needs to be trustworthy and should not compromise the assemblage data in any form. Data integrity is critical to maintaining trust in the assemblage. Trust needs to exist amongst all stakeholders involved in the ecosystem. It is vital to understand all the stakeholders so that each stakeholder can take responsibility for their actions. The stakeholders identified in the study include but is not limited to consumers, developers, device manufacturers, distributors, cloud providers, regulators, to name but a few.

The authors concluded that most consumers are unaware of the data collected by smart devices, stored data or even its intended usage. The consumer-level trust requires the consumers to understand the risks in using IoT devices. Consumers need to start asking questions before taking IoT devices to their home environments. While all stakeholders need to protect the consumers, the onus still lies with the consumers to ensure their safety by using trusted devices, trusted networks and data stored with trusted cloud providers.

If IoT devices are to connect to South African network operators, they need to be trustworthy. This will enable the fast adoption of CIoT in South Africa. Therefore, there should be a high level of trust between stakeholders.

Regulators such as the Independent Communication Authority of South Africa and the national broadcaster, the South African Broadcasting Cooperation, should ensure that IoT devices in the South African market are trustworthy. Global manufacturers that do not meet the South African safety requirements should not play a role in the South African market. The same rigour should apply to other stakeholders such as developers and cloud providers. The authority needs to empower itself to understand these issues.

At the network and storage level, the heterogeneity of protocols and smart devices enable new security threats in the CIoT assemblage. The authors recommend a speedy development of universal standards that manufacturers and other stakeholders can use. Some users have blind trust in global brands, hoping that all company policies should consider all trust concerns.

Acknowledgements

The authors would like to acknowledge Letitia Greenberg for language editing of the article.

Competing interests

The authors have declared that no competing interest exists.

Author's contributions

Mfanasibili Ngwenya and M.N. conceptualised the study. Mfanasibili Ngwenya conducted literature review and collected data. M.N. wrote the article and supervised the study.

Ethical considerations

The study was issued ethical clearance by UNISA College of Human Science Ethics Review Committee.

Funding information

This research received no specific grant from any funding agencies in public, commercial or not-for-profit sectors.

Data availability

Data are available on request.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any affiliated agency of the authors.

References

- Ali, M.S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F. & Rehmani, M.H., 2018, 'Applications of blockchains in the Internet of Things: A comprehensive survey & tutorials', *IEEE Communications Surveys* 21(2), 1676–1717. <https://doi.org/10.1109/COMST.2018.2886932>
- Ayaz, H., 2019, 'Advances in neuroergonomics and cognitive engineering', *Proceedings of the AHFE 2019 International Conference on Neuroergonomics and Cognitive Engineering, and the AHFE International Conference on Industrial Cognitive Ergonomics and Engineering Psychology*, Springer, Washington, DC, July 24–28, 2019, pp. 427–437.
- Babar, S., Mahalle, P., Stango, A., Prasad, N. & Prasad, R., 2010, 'Proposed security model and threat taxonomy for the Internet of Things (IoT)', *International Conference on Network Security and Applications*, Springer, Chennai, 23–25 July 2010, pp. 420–429.
- Biswas, K. & Muthukumarasamy, V., 2016, 'Securing smart cities using blockchain technology', *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, IEEE, Sydney, NSW, 12–14 December 2016, pp. 1392–1393.
- Braun, V. & Clarke, V., 2006, 'Using thematic analysis in psychology', *Qualitative Research in Psychology* 3(2), 77–101. <https://doi.org/10.1191/1478088706qp0630a>
- Braun, V. & Clarke, V., 2020, 'One size fits all? What counts as quality practice in (reflexive) thematic analysis?', *Qualitative Research in Psychology* 18(3), 328–352. <https://doi.org/10.1080/14780887.2020.1769238>
- Bryman, A., 2016, *Social research methods*, Oxford University Press, Oxford.
- Chen, D., Chang, G., Jin, L., Ren, X., Li, J. & Li, F., 2011, 'A novel secure architecture for the Internet of Things', *2011 Fifth International Conference on Genetic and Evolutionary Computing*, IEEE, Xiamen, 29 August – 01 September 2011, pp. 311–314.
- Chen, R., Bao, F. & Guo, J., 2015, 'Trust-based service management for social Internet of Things systems', *IEEE Transactions on Dependable and Secure Computing* 13(6), 684–696. <https://doi.org/10.1109/TDSC.2015.2420552>
- Cheng, X., Fu, S., Sun, J., Bilgihan, A. & Okumus, F., 2019, 'An investigation on online reviews in sharing economy driven hospitality platforms: A viewpoint of trust', *Tourism Management* 71, 366–377. <https://doi.org/10.1016/j.tourman.2018.10.020>
- Clandinin, D.J., 2006, 'Narrative inquiry: A methodology for studying lived experience', *Research Studies in Music Education* 27(1), 44–54. <https://doi.org/10.1177/1321103X060270010301>
- Creswell, J.W. & Poth, C.N., 2017, *Qualitative inquiry and research design: Choosing among five approaches*, Sage, Los Angeles.
- Crosby, M., Pattanayak, P., Verma, S. & Kalyanaraman, V., 2016, 'Blockchain technology: Beyond bitcoin', *Applied Innovation* 2, 6–10.
- Delanda, M., 2016, *Assemblage theory*, Edinburgh University Press, Edinburgh.
- Duranti, L., 2020, 'Of truth, evidence and trust: Records and archives in the era of misinformation and disinformation', in J.A. Bastian & E. Yakeel (eds.), *Defining a discipline*, 9p., Society of American Archivists, Chicago, IL, viewed 10 August 2020, from https://www.academia.edu/45523932/Of_Truth_Evidence_and_Trust_Records_and_Archives_in_the_Era_of_Misinformation_and_Disinformation_pre_print.
- Diamantopoulou, V., Androutsopoulou, A., Gritzalis, S. & Charalabidis, Y., 2020, 'Preserving digital privacy in e-participation environments: Towards GDPR compliance', *Information* 11(2), 117. <https://doi.org/10.3390/info11020117>
- Fong, L.H.N., Lam, L.W. & Law, R., 2017, 'How locus of control shapes intention to reuse mobile apps for making hotel reservations: Evidence from Chinese consumers', *Tourism Management* 61, 331–342. <https://doi.org/10.1016/j.tourman.2017.03.002>
- Gao, L. & Bai, X., 2014, 'A unified perspective on the factors influencing consumer acceptance of internet of things technology', *Asia Pacific Journal of Marketing and Logistics* 26(2), 211–231. <https://doi.org/10.1108/APJML-06-2013-0061>
- Hashemi, S.H., Faghri, F., Rausch, P. & Campbell, R.H., 2016, 'World of empowered IoT users', in *Proceedings of 2016 IEEE 1st international conference on internet-of-things design and implementation*, Institute of Electrical and Electronics Engineers Inc., Berlin, April 4–8, pp. 13–24.
- Jovchelovitch, S. & Bauer, M.W., 2000, 'Narrative interviewing', in M.W. Bauer & G. Gaskell (eds.), *Qualitative researching with text, image and sound*, pp. 57–74, Sage, London.
- Kiger, M.E. & Varpio, L., 2020, 'Thematic analysis of qualitative data: AMEE Guide No. 131', *Medical Teacher* 42(8), 846–854. <https://doi.org/10.1080/0142159X.2020.1755030>
- Laplante, P. & Applebaum, S., 2019, 'NIST's 18 Internet of Things trust concerns', *Computer* 52(6), 73–76. <https://doi.org/10.1109/MC.2019.2908544>
- Lee, I. & Lee, K., 2015, 'The Internet of Things (IoT): Applications, investments, and challenges for enterprises', *Business Horizons* 58(4), 431–440. <https://doi.org/10.1016/j.bushor.2015.03.008>
- Liebenberg, L., Jamal, A. & Ikeda, J., 2020, 'Extending youth voices in a participatory thematic analysis approach', *International Journal of Qualitative Methods* 19, 1609406920934614. <https://doi.org/10.1177/1609406920934614>
- Mollah, M.B., Azad, M.A.K. & Vasilakos, A., 2017, 'Security and privacy challenges in mobile cloud computing: Survey and way ahead', *Journal of Network and Computer Applications* 84, 38–54. <https://doi.org/10.1016/j.jnca.2017.02.001>
- Ngoepe, M. & Ngwenya, M., 2022, 'Personal data and the assemblage security in consumer Internet of Things', *International Journal of Information Security and Privacy (IJISP)* 16(1), 1–20. <https://doi.org/10.4018/IJISP.2022010108>
- Ngwenya, M., 2020, 'Data privacy, security and trust in consumer internet of things' assemblages and associated mobile applications in South Africa', PhD thesis, University of South Africa, Pretoria.
- Ouaddah, A., Abou Elkalam, A. & Ait Ouahman, A., 2016, 'FairAccess: A new blockchain-based access control framework for the Internet of Things', *Security and Communication Networks* 9, 5943–5964. <https://doi.org/10.1002/sec.1748>
- Palattella, M.R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T. et al., 2016, 'Internet of Things in the 5G era: Enablers, architecture, and business models', *IEEE Xplore* 34(3), 510–527. <https://doi.org/10.1109/JSAC.2016.2525418>
- Pilkington, M., 2016, 'Blockchain technology: Principles and applications', in F.X. Olleros & M. Zhugu (eds.), *Research handbook on digital transformations*, pp. 225–253, Edward Elgar Publishing Limited, Cheltenham.
- Rose, K., Eldridge, S. & Chapin, L., 2015, *The Internet of Things: An overview*, pp. 1–50, The Internet Society, viewed 15 March 2020, from <https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf>
- Sadeghi, A.-R., Wachsmann, C. & Waidner, M., 2015, 'Security and privacy challenges in industrial internet of things', *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE*, San Francisco, CA, IEEE, 8–12 June 2015, pp. 1–6.
- Scârnci-Domnişoru, F., 2013, 'Narrative technique of interviewing', *Bulletin of the Transilvania University of Braşov, Series VII: Social Sciences and Law*, 6(55), pp. 21–28, viewed 18 April 2020, from <http://webbut2.unitbv.ro/bu2013/Series%20VII/BULETIN%20VII%20PDF/05%20Scârnci-Domnişoru.pdf>
- Schmitt, C., Meier, J., Diez, M. & Stiller, B., 2018, 'OTIoT – A browser-based object tracking solution for the Internet of Things', *Internet of Things (WF-IoT), 2018 IEEE 4th World Forum on*, 2018, IEEE, Singapore, pp. 445–451.
- Sivarajah, U., Kamal, M.M., Irani, Z. & Weerakkody, V., 2017, 'Critical analysis of Big Data challenges and analytical methods', *Journal of Business Research* 70, 263–286. <https://doi.org/10.1016/j.jbusres.2016.08.001>
- Skulmoski, G.J., Hartman, F.T. & Krahn, J., 2007, 'The Delphi method for graduate research', *Journal of Information Technology Education: Research* 6, 1–21. <https://doi.org/10.28945/199>
- Tchernykh, A., Schwiigelsohn, U., Talbi, E.-G. & Babenko, M., 2016, 'Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability', *Journal of Computational Science*, 36, 100581. <http://dx.doi.org/10.1016/j.jocs.2016.11.011>

Tiwary, A., Mahato, M., Chidar, A., Chandrol, M.K., Shrivastava, M. & Tripathi, M., 2018, 'Internet of Things (IoT): Research, architectures and applications', *International Journal on Future Revolution in Computer Science Communication Engineering* 4, 23–27.

Want, R., Schilit, B.N. & Jenson, S., 2015, 'Enabling the Internet of Things', *Computer* 48(1), 28–35. <https://doi.org/10.1109/MC.2015.12>

Yan, Z., Zhang, P. & Vasilakos, A.V., 2014, 'A survey on trust management for Internet of Things', *Journal of Network and Computer Applications* 42, 120–134. <https://doi.org/10.1016/j.jnca.2014.01.014>

Zyskind, G. & Nathan, O., 2015, 'Decentralizing privacy: Using blockchain to protect personal data', *Security and Privacy Workshops (SPW), 2015 IEEE*, San Jose, CA, 21–22 May 2015, IEEE, pp. 180–184.