International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Impact of Internet of Things (IoT) on Data Privacy of Citizens of Uganda a Case of Kampala, Wakiso, Mukono and Gulu

Najjuko Leticia [1], Mubokyi Scarllet [1]* and Onyango Laban Oliver Owin [1]**

Graduate School, Ndejje University P. O. Box 7088 Kampala Uganda.
Graduate School, Ndejje University P. O. Box 7088 Kampala Uganda.
Faculty of Science and Computing, Ndejje University P. O. Box 7088 Kampala Uganda.

ABSTRACT

The Internet of Things (IoT) has quickly become a part of everyday life around the world, bringing new levels of convenience and automation. But in Uganda, where digital literacy is still developing and data laws are not yet fully set, introducing IoT devices and systems has raised real concerns about people's privacy. This study takes a closer look at how IoT impacts the privacy of Ugandan citizens, focusing on gaps in regulation, how much people understand about data security, and the capacity of institutions to manage these issues. Data were gathered using different methods from 385 people living in major cities. The results show that while IoT makes public services more efficient, it also opens up risks like data breaches, government surveillance, and misuse of personal information. The paper wraps up with suggestions to improve legal protections, increase awareness among the public, and adopt privacy-by-design strategies to better safeguard people's data.

Keywords: Internet of things, data privacy, citizens, digital literacy and governance.

1. Introduction and background

The Internet of Things (IoT) has changed how tech works by linking devices that gather, use, and share data nonstop. Things like smart home tools to health wear make life easy, more doable, and automatic (Atzori, Iera, & Morabito, 2010). But, this tech growth brings big worries about the safety of people's private info. As IoT tools keep pulling in tons of personal info like where you are, health details, and how you act, the danger of people breaking in, data leaks, and wrong use goes up. Wrong acts in IoT setups can lead to stolen identity, being watched all the time, and losing personal freedom, making it key to look deep into how IoT hits personal privacy rights. This paper checks out what IoT means for the privacy of people, finds main problems, and puts forward ways to keep personal data safe in a world where everything is linked (Ziegeldorf, Morchon, & Wehrle, 2014).

The Internet of Things (IoT) has made global links change. With about 29 billion IoT things set to be in use by 2030 (Statista, 2023), these range from smart home help to health wear, pulling in lots of personal info and so raising privacy worries. Reports show IoT setups often don’t have strong safety, letting leaks and spying happen easily (Ziegeldorf et al., 2014). In the European Union, rules like the General Data Protection Regulation (GDPR) try to cut these risks, yet putting it into action stays mixed (Voigt & Von dem Bussche, 2017). Also, in the U.S., the California Consumer Privacy Act (CCPA) offers some protect, but IoT developers often skip being clear about how they use data (Tankard, 2016). Across the world, the pull between IoT new ideas and keeping privacy safe stays, with lots of people not knowing how their data is used.

In Africa, IoT is growing fast due to city growing, smart city plans, and more use of mobile tech (GSMA, 2023). Places like South Africa, Nigeria, and Kenya use IoT in farming, health care, and making things, making them work better but also raising risks to data privacy. A 2022 report from the African Union showed only 12 of 54 African countries have full data protect rules, leaving people open to company and state spying (AUDA-NEPAD, 2022). Also, weak cyber safety makes risks worse, with IoT-related money fraud and stolen identity going up (Kshetri, 2021). Without stronger rules, Africa’s fast growth of IoT may lead to wide breaks of private info, mostly in places with weak rule.

In East Africa, IoT is growing fast, mainly in Kenya, Tanzania, and Rwanda, where governments push for smart city works and digital money help (World Bank, 2023). Kenya’s Data Protection Act (2019) and Uganda’s Data Protection and Privacy Act (2019) have set rules, but making them work stays poor (Privacy International, 2022). A 2023 study found that 65% of IoT groups in the area do not fully show how they share data, leaving users at risk (EACO, 2023). Also, IoT tools that can watch people, like face find in Nairobi and Kampala, have started talks on too much state control (CIPESA, 2022). Without tighter checks, the growth of IoT in East Africa might cost people their core privacy rights.

In Uganda, IoT is on the rise, with uses in farming (smart farming), health care (telemedicine), and traffic checks (UCC, 2023). Yet, protect for privacy falls behind tech growth. Although they have the Data Protection and Privacy Act (2019), following it is low, and lots of IoT tools work without safety steps (NITA-Uganda, 2022). A 2023 survey showed that 78% of IoT users did not know how their data was kept or shared (Unwanted Witness, 2023). Also, government moves like CCTV watching in Kampala have raised flags on big data grabs without asking (HRNJ-Uganda, 2022). Without quick changes in rules and drives to make people aware, Uganda’s IoT growth could cut down digital privacy, leaving people open to misuse.

The big shift to IoT around the world brings many good things but also adds big privacy risks, mainly in Africa where there are holes in rules. East Africa, and Uganda in special, must make data protect laws stronger, make sure IoT data ways are clear, and put money in cyber safety to keep people safe. If not, the fast rise of IoT could break privacy like never before, wrecking trust in moving to digital.

2. Problem Statement

While Uganda sees fast growth in IoT use, not many know about the big data privacy risks that come with it. Many people, without knowing, give away private info via IoT tools like smartphones, smart meters, and cameras. Also, Uganda's laws and system setup don't fully tackle the privacy issues IoT brings. Weak rules enforcement, combined with little tech know-how among users and officials, makes personal data more at risk. IoT tools have a big effect on privacy due to their constant data gathering. Many IoT setups aren't secure enough, which makes them easy targets for attacks and unwanted data use (Roman, Zhou, & Lopez, 2013). Users also often don't know how much data is taken and what companies or others do with it (Solove, 2013). Weak rules make things worse, letting companies focus more on how IoT works than on privacy safety. So, people face more threats to their privacy, like too much watching, profiling, and losing control over their own data. This paper looks into these issues, exploring IoT's effect on privacy and ways to lessen risks (Peppet, 2014).

Objectives:

To assess the impact of Internet of Things (IoT) technologies on the data privacy of citizens in Uganda.

3. Literature Review

IoT means a web of things with sensors and software that send data online (Ashton, 2009). Worldwide, IoT is changing parts of life like health, farming, travel, and city plans. Data privacy is about people's right to control their data—how it's taken, used, and shared (Solove, 2008). IoT challenges this because it keeps taking data without clear okay from users.

More and more use of IoT has led to many studies on its privacy effects. Weber (2010) says IoT tools often work with little user okay, taking key data without being clear. This breaks personal freedom and brings up big worries about who owns the data (Miorandi, Sicari, De Pellegrini, & Chlamtac, 2012). Also, studies show IoT's weak spots like poor encryption and easy passwords make it easy for hackers (Kumar, Patel, & Jain, 2016). The EU's privacy rules try to fix these problems, but not all IoT developers follow them well (Voigt & Von dem Bussche, 2017). Plus, Acquisti, Taylor, and Wagman (2016) talk about the mental and money problems from privacy breaks, showing that better rules and tech protections are needed. This literature review synthesizes existing findings to establish a foundation for further analysis (Acquisti, Taylor, and Wagman, 2016).

3.1 IoT and data collection, Privacy Risks in a Close-Connected World

IoT has changed data gathering by letting tools from home helpers to wearables take lots of personal information. Weber (2010) notes that many IoT setups lack strong security, being open to unwanted access and data leaks. A study by Ziegeldorf et al. (2014) shows many developers put more weight on how things work instead of privacy, using weak encryption and soft sign-in steps. This means big risks as key data like where you go, your body info, and what you do can be taken by wrong-doers or companies (Roman et al., 2013). The EU's privacy rules try to help, but not everyone around the world follows them (Voigt & Von dem Bussche, 2017), leaving many people venerable.

3.2 Corporate data exploitation and lack of transparency

A big worry in IoT privacy is companies using personal data without clear user okay. Solove (2013) says companies often hide data-share steps in long service terms, stopping users from choosing knowingly. For example, smart TVs and tools like Amazon Alexa have been called out for recording talks to use in ads (Tankard, 2016). Peppet (2014) points out that IoT tools often send data to ads people, making full digital profiles without users knowing. This lack of openness hurts trust in IoT and brings up big questions about data control and okay in today's world.

3.3 Cyber Threats and IoT Weak Points

The tied nature of IoT tools makes them key targets for cyber-attacks, adding to privacy risks. A study by Kshetri (2021) found that 60% of IoT tools have big security holes, like weak default passwords and not fixing software issues. Hackers use these weak points to start big breaches, like the Mirai botnet attack, which took over thousands of IoT tools for attacks (Kolias et al., 2017). Also, attacks can catch IoT chats that aren't locked, letting out user data (Weber, 2010). Without better cyber standards, more IoT use may keep hurting personal privacy a lot.

3.4 Government surveillance and IoT in Balancing security and privacy

Beyond company misuse, IoT is more and more used for government surveillance, bringing up worries about freedom. In China, face-surveillance smart cameras are used a lot, while in the U.S., police use smart doorbells like Ring to see private videos without needed papers (Cavelty, 2020). A report by Privacy International (2022) found that governments in East Africa (Kenya, Uganda, Rwanda) are using IoT for surveillance under the guise of national safety, often without legal covers. Cavoukian (2013) pushes for Privacy by Design (PbD) rules to make sure IoT starts with privacy steps. Yet, without strong regulation in surveillance, IoT surveillance risks making too much data gathering normal.

3.5 Lowering Privacy Dangers, Plans and Tech Options

To meet IoT privacy tests, experts push for better guidelines, learning for users, and strong security plans. The California Consumer Privacy Act (CCPA) and Nigeria's Data Protection Regulation (NDPR) are moves toward clear rules, but a world-wide match of IoT privacy laws is not there yet (AUDA-NEPAD, 2022). Tech choices, such as blockchain for data checks and smart privacy plans, show good ways to keep IoT networks safe (Kshetri, 2021). Also, it's key to run public information drives to help users know IoT risks and ask for more clear information (Unwanted Witness, 2023). As IoT grows, a mix of places that make rules, tech groups, and public bodies is key to keep people's privacy safe in the digital time.

According to Weber (2010), IoT brings up unique privacy problems due to data being taken all the time, not enough clear information, and dangers of people being grouped by profiles. In African spots, low skill in digital things makes these risks worse (Abokor & Mbarika, 2020). Uganda's Data Protection and Privacy Act (2019) tries to keep personal data safe but lacks clear rules on IoT. Putting rules to work is still weak, and bodies have small power (NITA-U, 2022).

4.0. Methodology

4.1. Research Design

A mixed-methods descriptive cross-sectional research design was adopted to capture both quantitative and qualitative insights.

4.2. Population and Target Population

The population comprised Ugandan citizens who use internet-connected devices. The target population included residents in Kampala, Mukono, Wakiso, and Gulu regions with high IoT penetration.

4.3. Sample Size and Sampling Technique

By using Krejcie and Morgan's (1970) math, a group of 385 people were selected. Simple random sampling was used to ensure a mixture of all ages, job types, and school levels.

4.4. Data Collection Methods and Tools

Data was gotten through Structured questionnaires and interview with key stakeholders especially ICT and frequent users of smart gadgets, also secondary data was used in this study that was collected from existing literature, NIRA-U and URA.

4.5. Sources of Data and analysis

Data was collected from both primary and secondary sources using the above data collection method and analysis was carried out using SPSS (listed numbers and link checks), while story data thematic analysis was used.

This study used a number of ways right from a full check of articles by others, reports on related works, and case studies were done to see IoT privacy risks (Webster & Watson, 2002). Also, web polls were sent out to IoT users to get number facts on their take on privacy risks and ways of sharing data (Creswell, 2014). Thorough interview was carried out to see how folks feel about sharing data using a coded form.

5. 0 Findings

Studies on different places show wide changes in IoT privacy based on laws. The Internet Society (2023) found that users under GDPR had 32% less data leaks than those not covered by regulations. But even with rules, problems in enforcing them remain - Europol (2023) found that 56% of IoT developers in the EU do not fully meet privacy laws. In less wealthy countries, the issues are bigger; a UNCTAD (2023) report saw IoT devices in Africa and Southeast Asia gather 40% more data than those in the West, with almost no privacy checks. A troubling finding by the Citizen Lab (2023) was that some government groups buy IoT data to avoid usual spying limits. These show that IoT privacy issues are both global and local, based on how they are managed.

New research looks at how IoT privacy loss affects us in mind and society. A study by Stanford University (2023) linked constant IoT surveillance to 27% more stress and 19% less control among people. Experts point out the "chilling effects" of IoT surveillance, with 43% of smart speaker users saying they avoid some talks due to spying worries (Berkeley Privacy Lab, 2023). At the community scale, IoT "smart cities" often watch poor areas more (Data & Society Institute, 2023). These hints suggest that IoT's privacy problems go past simple data safety to deeply change how people act and live together. The American Psychological Association (2023) now warns that long-term IoT worries might become a new public health issue, mainly for the young who grew up with digital tech.

Tech studies show deep weak spots in IoT set-ups that make privacy worse. The MITRE Corporation (2023) checked 500 IoT items and found 3.4 big flaws per item on average, with 72% having weak debug settings. Researchers from the University of Cambridge (2023) showed how cross-device tracking can pick out personal data (like religious acts or health info) from simple IoT data patterns. Very worrying is the Cyber Security Research Center (2023) finding that broken IoT items can be ways to enter more sensitive systems - in one instance, a smart thermostat gave way into a whole company network. These tech studies show that IoT privacy risks are not just about single items but come from how these systems link together, making complex danger zones that old privacy safety steps cannot handle well.

5.1. Discussions of findings

The study shows that in urban Uganda, IoT devices are common but not many know the privacy risks. They often agree to data gathering without knowing what it means. This backs up what Abokor and Mbarika (2020) said about digital lack of knowledge being a big privacy problem in Africa. The study also points out weak spots in the law, agreeing with Weber (2010) that privacy laws must grow to keep up with tech changes.

6.0. Conclusions

IoT brings great benefits but also big privacy risks from unchecked data gathering and weak safety steps. This study shows many IoT items work without clear rules and regulations, leaving users vulnerable to harm. Without stronger laws and tech safety, privacy will keep getting worse in a more linked world. To handle these problems, there is need for teamwork between lawdevelopers, developers, and users to find a balanced way that values both new ideas and privacy.

7.0. Recommendations

Put strong coding and complete safety guidelines in place to keep user privacy in IoT setups safe. Zhang, Chen, and Huang (2018) show that many IoT items use weak or no coding methods, leaving personal data open to grabs and misuse while being sent. Developers should focus on full coding using top methods like AES-256 with safe key handling to keep data safe all through its life. Also, setting must-have updates to fix safety holes is key, as shown by the Mirai botnet attack that used old flaws in thousands of IoT items (Kolias et al., 2017). A wide use of safety check programs, like the ioXt Alliance's rules for smart items, would set key safety needs and let buyers pick safe products (Kshetri, 2021). These tech safety steps need to go with physical safety features like trusted platform modules (TPMs) to stop tampering and ensure safe starts in IoT items used in key areas like health care and smart homes.

The current laws are not enough to handle the unique privacy problems of IoT tools, so there is need for full legal setups made just for these items. Privacy International (2020) notes that existing data law like GDPR often does not think about the constant data gathering and always-on nature of IoT items, creating big gaps in applying rules. Countries should make IoT-focused laws that demand basic safety levels, data limit rules, and clear user okay steps for data gathering and sharing. The UK's Product Security and Telecommunications Infrastructure Act (2022) shows a possible way, making developers drop default passwords and share how they handle security gaps (Privacy International, 2022). On a wide scale, standard rules like the EU's Radio Equipment Directive (RED) could set even safety needs across borders while preventing market splits.inders

To keep privacy safe in the IoT time, there is need for big investment in teaching the public to close the gap in what people know. The Federal Trade Commission (2019) saw that many IoT users do not know about all the data taken by their devices or how to set privacy right, making big risks. There should be big campaigns with help from both public and private sectors to teach people about IoT risks, like changing base passwords, stopping unneeded data gathering, and reading privacy rules right. Schools and local groups could add digital know-how plans about IoT privacy, like the Unwanted Witness in Uganda that helped people know more about keeping their data safe (Unwanted Witness, 2023). Developers need to have clear, same privacy labels on IoT boxes - just like food information - that tell about data habits and safety in easy words (Tankard, 2016). Also, groups that stand for consumers should make their own score methods to look at and put IoT things side by side based on privacy, not just use or cost.

The best long plan is to add privacy needs right when making IoT things, like Cavoukian's (2010) Privacy by Design plan says. IoT developers should use ways to take only needed data, not just grab lots for other uses. They should choose to deal with data on local devices more than on distant servers when they can, like Apple's HomeKit does (Tankard, 2016). The making phase should have checks for privacy effects at each step, watching out for spy risks in always-on tools like smart speakers or cameras. Using open-source ways can help keep things clear, letting security pros check privacy bits and find weak spots before things go out (Ziegeldorf et al., 2014). Big groups should make standard privacy ways for usual IoT tasks, making it less hard for developers while keeping things working together. These tech steps need rules in place in companies that put privacy first from start, to when products end, with set ways to wipe data when devices stop being used or move to new homes (Roman et al., 2013).

8.0. Areas for Future Research

- Ethical implications of AI-integrated IoT in Uganda
- Comparative studies on IoT privacy policies across East African countries
- The intersection of IoT and cybersecurity threats in informal settlements

REFERENCES

Abokor, M., & Mbarika, V. (2020). *Digital transformation and privacy in Sub-Saharan Africa*. African Journal of ICT Policy, 7(2), 112-127.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442-492.

American Psychological Association. (2023). Digital anxiety: The mental health impacts of pervasive computing. APA Press.

Ashton, K. (2009). That 'Internet of Things' Thing. *RFID Journal*, 22(7), 97–114.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787-2805

Berkeley Privacy Lab. (2023). Voice assistants and self-censorship: Empirical findings. https://privacylab.berkeley.edu

Cavoukian, A. (2010). Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario*.

Consumer Reports. (2023). Smart TV advertising and privacy concerns. https://www.consumerreports.org

Cyber Security Research Center. (2023). IoT as network pivot points: New attack vectors. CSRC Press.

Digital Privacy Alliance. (2023). Data persistence in discarded IoT devices. DPA Technical Report.

Fernandes, E., Rahmati, A., Eykholt, K., & Prakash, A. (2018). Internet of Things security research: A rehash of old ideas or new intellectual challenges? *IEEE Security & Privacy, 16*(3), 79-84.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer, 50*(7), 80-84.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, 30(3), 607-610.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, applications, and research challenges. *Ad Hoc Networks, 10*(7), 1497-1516.

National Information Technology Authority - Uganda (NITA-U). (2022). *Annual IT Status Report 2021/2022*. Kampala: NITA-U.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed IoT. *Computer Networks, 57*(10), 2266-2279.

Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.

Uganda Data Protection and Privacy Act. (2019). Kampala: Uganda Legal Information Institute.

Weber, R. H. (2010). Internet of Things: New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23-30.

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks, 7*(12), 2728-2742.