The Efficiency of a framework to Enhance Confidentiality and Privacy of Data inMotion

[1] Ahamya William, [2]Drake Mirembe and [1]Evarist Nabaasa
[2]College of Computing and Information Sciences, Makerere University
[1]Mbarara University of Science and Technology

Abstract

Using a descriptive cross-sectional research design, this study sampled 44 participants comprised of top managers and directors; experts in car tracking and sensor installers, and FMS Clients. Data was collected using structure questionnaires and analyzed quantitatively. Various analysis and test including correlation and regression were conducted. The findings revealed that there is a significant relationship between consent and the effectiveness of the designed framework of data in motion (r=.686**); implying that consent enhance trust and honesty, and empower the users to have the final say onwho retrieves their data unlike before when the service provider and other third parties would without seeking permission from the client. It was noted that there is a significant effect of confidentiality on the effectiveness of the designed framework of data in motion (r=.342**). This implies that anonymity of the users shall build trust, protects reputation and prevents misuse of confidential data. Study findings noted that there is a significant effect of privacy on the effectiveness of the designed framework of data in motion (r=.589**). This implies that in privacy, there is respect for individuals reputation and movement, enhance trust and individuals has a reasonable desire to keep something private. Undertaking mediation and interaction effects amongst variables and well as establishing the longitudinal results of the relationship between study variables are recommended in further studies.

1.0 Background and Contextual

The growing interested of realizing value personal security, privacy, confidentiality and human rights, has made scholars to pick interest on the privacy and confidentiality is vital and uncompromised both at motion and at rest. Henceforth, to add to the growing scholarly debate in this dominion, this research was set out. That is, it was set out to explore the efficiency of the designed framework of data in motion in Uganda.

Data in motion also referred to as data in transit, is digital information transferred between locations either within or between computer systems (Berecki, 2019). Employees are often using multiple devices to get their work done, and this means that information is being created and shared in diverse ways across various locations. Data in motion must be safeguarded not only because of a growing number of regulatory guidelines, but to avoid exposure to possible financial penalties as well as reputational risks (Kagita, Thilakarathne, Rajput & Lanka, 2020).

World-over, as data network infrastructure is the on-ramp for all institutions' connectivity, the threat to intellectual property, government secrets, sovereignty, citizen identities and critical national infrastructure have never been greater. Today's businesses are focusing on how harness the power of huge volume of streaming data to improve operations and become more agile (Oppitz & Tomsu, 2018). Data in motion is also vital to those working in big analytics, as the processing of data can help an institution analyze and gain insight unto trends as they occur. However, data in motion is exposed to many risks; as data travels, both inside and outside the company, it can easily fall into the wrong hands (Wlosinski, 2018). When in motion, data has to contend with wide range of threats, including network failures, human error, insecure file sharing, malicious actions, and more.

Interestingly, there is undoubtedly a continuous growing security concern over the exposure of information and data in motion. The privacy and confidentiality of users have not been full respected (Ettredge, Guo & Li, 2018). The rise of shadow IT also leads to increased possibilities of sensitive data being leaked, as it can be easily transmitted to persons outside the company. In recent years, with the rapid development of video surveillance infrastructure, more and more intelligent surveillance systems have employed computer vision and pattern recognition techniques. Dashboard cameras can provide video evidence in the event of the road accident or vandalism (Abaho, 2017). For this reason, numerous cars

are now equipped with dashboard cameras and, in a number of countries, dashboard cameras are mandatory on public transport, such as buses and taxis. License plate number is also a unique sign of the vehicle, so license plate recognition is an important part of vehicle recognition in modern intelligent surveillance systems (Abaho, 2017). Car tracking based on surveillance videos suffers from poor quality and significant installation costs limiting its applicability. Conceptually, the research improved on seeking consent, privacy and confidentiality of data in motion in embeddedsystems as illustrated in the Figure 1.1:

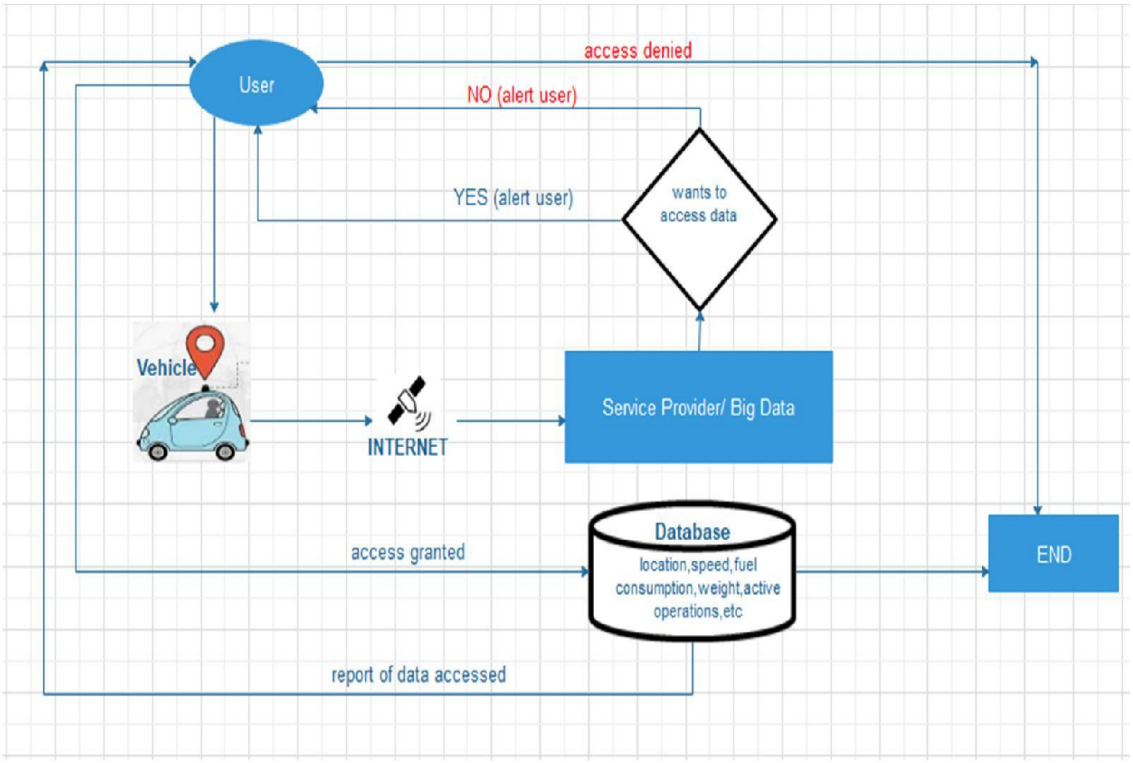

Figure 1.1: **Showing data flow in the designed modified framework**

From this illustration in Figure 1.1 above, data in motion is commonly transmitted from the sensors embedded in the car and sentto the internet through the IoT gateway. Despite, the existing framework doesn't empower the user to have the final say/decision on who retrieves their data. Sending sensitive information through work stream collaboration platforms like Slack or Mattermost can easily expose it orsend it into the wrong hands (unauthorized users), whether inside or outside the organizationhence leading to data misuse(Ettredge *et al.,* 2018). Commonly the service providers and other third parties can access or retrieve data in motion without prior warning or seeking consent from the

user. Service providers do not forward a notification to users in case assessing data or tampering with it, by whom and at what time (Kagita et al., 2020).

Moreover, the current solutions that have been proposed by the government still face major challenges. For example, the intrusive application of surveillance of logs harms the right to privacy of Ugandans. This contravenes with the rule of law where privacy is a fundamental right enshrined in the 1995 Constitution and numerous international human rights treaties and other legal instruments. The right to privacy is also a central pillar of a well-functioning democracy (Mukasa, 2021). GPS controllers always have access to the car driver movements without his/her consent or notification which eventually interfere with one's privacy and security (Katushabe, 2021). Regrettably, all these have hitherto remained mere allegation without systematic answers to the predicament. This prompted the current researcher to consider the path of the research study.

2.0 The Problem Statement

The data in motion is becoming the currency in this global village. The privacy and confidentiality is vital and uncompromised both at motion and at rest. The accuracy and valid (consistent) of designed framework of data in motion is effective towards theft protection, and help law enforcement to identify and apprehend alleged perpetrators (Abaho, 2017). It boasts sophisticated monitoring capabilities, and helpful analytics to extend your vehicle's longevity and improve safety, including driver whereabouts, and vital diagnostics, such as critical feedback on fuel consumption, oil, tire pressure and other concerns (Mukasa, 2021).

However, various service providers have and continue gaining unauthorized access and misuse of data in motion and at rest from embedded systems for nefarious activities. The maincauses of data breaches includes, negligent workers or contractor (48%), third party mistakes (41%), external attacks (27%), and malicious insider (5%), that access data without consent thus inflicting users' privacy, trust and confidentiality (Katushabe, 2021). Still, with presence of surveillance of logs, the privacy and guaranteeing of security to car drivers have not been granted henceforth undermining human rights. Consequently, this research sought to establish the efficiency of the designed framework of data in motion.

Therefore, to fulfill this research gap, the following research objectives hereunder to guide this research:-

1. To analyze the correlation between consent and efficiency of the designed framework of data in motion.
2. To ascertain the relationship between confidentiality and efficiency of the designed framework of data in motion.
3. To find out relationship between privacy and efficiency of the designed framework of data in motion.

3.0 Literature Review

3.1 Consent and Effectiveness of the Designed Framework of Data in Motion

According to Berecki (2019), one prudent approach to minimize the potential for harm is to gain informed consent from individuals who are disclosing data. With the increasing presence of (and reliance on) digital technologies, it is critical for individuals to understand what they are consenting to by sharing data. As the capabilities of data analytics push further ahead, the risks grow for those whose data is gathered. The likelihood that previously anonymized data may become de-anonymized increases with each new advance (Abaho, 2017). Inherent biases are introduced through algorithm selection, training data, and hypothesis testing, which can result in automated decision-making that is biased. Informed consent is vital because it build a relationship of trust between the individual and the managers which then makes it easier for the individual to be honest. They also relieve stress and make individual car users to feel more autonomous. Data in motion is exposed to many risks; as data travels, both outside and inside an organization, it can easily fall into the wrong hands.

Similarly, it's vital to help designers and developers minimize unintended harm from the use of that data. Ethical behaviours in this context are about the protection, treatment and transformation of data moving between systems (data in motion), not just recorded, static data (data at rest). Surprisingly, service providers and other third party need to seek consent from the users to access the data (Kagita *et al.,* 2020). Users should be empowered to have the final say onwho retrieves their data unlike before when the service provider and other

third parties wouldwithout seeking permission from the client. The algorithm is also sought to forward a notification to clients/ users about any data that was accessed or tampered with, at what time,and by whom (Katushabe, 2021). Due to the digitalization of businesses and the increased mobility of workers,data travels more and more to enable collaboration. The failure to protect and secure confidential data may not only lead to the loss of clients or business, but it also unlocks the dangers of confidential data being misused to commit illegal activity such as fraud. Thus, data in motion must be safeguarded not only because a growing number of regulatory guidelines; but require it in specific ways. Unprotected sensitive data can cause damages on several levels to an organization, including exposure to possible financial penalties and reputational risks.

3.2 Confidentiality and Efficiency of the Designed Framework of Data in Motion

According to Ettredge *et al.,* (2018), data confidentiality refers to protection of data from unauthorized access and disclosure, including means for protecting personal privacy and proprietary information. Confidentiality is one of the three dimensions of information security i.e. confidentiality, integrity and availability commonly called, the C-I-A triad. These threecharacteristics are not necessarily connected or dependent on each other, however, if there is problem occurring in any part of this triad, the others are consequentially affected. Data should always be encrypted when it's traversing any internal or external networks; and this includes encrypting all data prior to transport or using protected tunnels such as SSL/TLS or HTTPS.

More so, confidentiality guarantees that only authorized parties or processes with sufficient privileges access the information while Integrity ensures that data is only created modified or deleted by authorized parties and availability ensures that data can be accessed in a timely and reliable way when people or applications need it (Berecki, 2019). These three attributes can also be considered goals or objectives of information security since they together represent three very desirable properties of information system. However, the biggest risk for data in motion is sending confidential data-maliciously or inadvertently, to someone who has no legitimate access to it or sharing it publicly.

In this regards, performing strong identify verification ensure devices in motion are not compromised. In trying to effectively dispatch, track and control a dispersed fleet of vehicles and workers can be a daunting task (Wlosinski, 2018). With an all-satellite GPS solution

from GPS trackers, one is able to provide their clients with real-time information on the location and status of all assets and operators. Equally vital, one may directly communicate with the operator to efficiently and quickly adjust schedules and stops to minimize wasted resources and time. Todays, more and more private data and security information are stored in smartphones, thus the risk of data leakage is becoming a major concern for the information society.

In addition to prevent data theft and forgery, identity verification plays a vital role in speeding up online transaction process. Thus, by implementing digital identity verification solutions, organization can minimize the impact of fraud, protect sensitive data, and bolster their brand's reputation in motion (Kagita *et al.,* 2020). Confidentiality controls protect against the unauthorized use of information already in the hands of an organization, whereas, privacy protects the rights of an individual user to control the data that the organization collects, maintains and shares with others. Most often, security breaks occur not as the result of a sophisticated technical failure but as the result of a mistake made by someone with authorized access to data in motion.

3.3 The Privacy and Effectiveness of the Designed Framework of Data in Motion

The privacy is one of the core concepts of cyber security. Privacy ensures that secret data in motion is protected from unauthorized disclosure. Thus, protecting privacy is a responsibility shared between technologists and everyone else in the organization (Abaho, 2017). Clearly, cyber-security professionals and other IT experts bear the burden of ensuring that confidentiality controls are in place and functioning properly enhancing confidentiality and privacy of data in motion in embedded systems save losses financially. The access controls of data in motion are the main mechanisms used to enforce integrity requirements. Thus, availability ensures that data is available for use by authorized individuals at the time they need it. Violations of availability may occur as a result of intentional attacks, such as the denial of service attack that crippled the organization motion management system (Mukasa, 2021). Privacy requiremnets dictate the types of authorization granted to data, whereas, confidentiality controls ensure that people and suystems meet those privacy obligations. Many organizations adopt privacy policies based on their own ethical sense of

proper data handling. It prevents misuse of confidential data and protects organization reputation.

2.4 Challenges Associated with Data Privacy and Confidentiality

Despite the countless benefits provided by embedded systems, it is no secret that they pose many attractive attack vectors for various bad actors that may seek to gain access to user datain motion thereby using it for nefarious activities (Haber & Rolls, 2020). In the same premiseof data being intercepted when in motion, the triple constrain of data security (confidentiality, integrity and availability) are essentially compromised. Importantto note is that, this study focused majorly on reliability and trustworthiness of data becausefor confidentiality to be compromised, data would have ceased to be confidential as well as being available to unauthorized users.

Although, modern cryptography has enabled the embedded software to provide a relatively robust defense against "conventional" attacks that target basic security requirement such as confidentiality or integrity, more efforts are still needed at higher levels to protect the embedded software from a large diversity of attacks which exploit their development defectsessentially caused by implementation bugs or design flaws (Lu & Xu, 2019). Considering such threats is as important as the need to integrate hard-to-break mechanisms that meet functionalsecurity objectives, because the embedded system's strength depends on the easiest way to attack it, and this latter is mostly done through a discovered design or implementation shortcoming (Manickam *et al.,* 2019). Most existing frameworks like the Hadoop as argued do not provide the users with option of consenting to information being tapped or accessed from them either at rest or in transit hence the need for this proposed framework.

4.0 Methodology

The study used a descriptive cross-sectional survey design. It also employs a descriptive statistics due to the need of making inferences about possible relationships between variables. The study used quantitative approach. The target population included; top managers and directors; experts in car tracking and sensor installers, and FMS Clients, all equivalent to 44 respondents, and these were selected basing on Morgan and Krejcie (1970) table. Simple

random sampling was used in selection of respondents. Questionnaires were used in data collection. Data was majorly analyzed quantitatively.

5.0 Results

The findings of the survey are presented thematically below.

5.1 Respondent's Profile

5.1.1 Gender

The results in the table below were generated to explore the distribution of the gender of the respondents.

Table 1: Gender of the Respondents

	Frequency	Percent
Male	30	68.5%
Female	13	29.5
Total	44	100.0

Source: Primary data (2023)

From table above, findings indicated that the majority of the respondents were male constituting 68.5% compared to their female counterparts representing only 29.5% in the sample. This therefore implies that male respondents were more than the female respondents working and using car tracking systems in Kampala.

5.1.2 Age Group

Table 2: Age bracket

Age group	Frequency	Percent
18-27yrs	12	27.3
28–37yrs	14	31.8
38yrs and above	18	40.9
Total	**44**	**100.0**

Source: Primary data (2023)

Results from the above table 2 revealed that majority of the respondents 40.9% belong to age group of 38years and above, followed by age group between 28-37 year constituting 31.8%, and finally 18-27 years constituting 27.3%.

5.3 Duration in Tracking System

Table 3: The period have been using working or tracking system

Period	Frequency	Percent
Less than 5 years	26	50.1
6 – 10yrs	12	27.3
11 yrs. & above	6	13.6
Total	**44**	**100.0**

Source: Primary data (2023)

Results from above show that majority of the respondents 50.1% have been using tracking system for a period of less than 5 years, 27.3% of respondents have been using tracking system for 6-10 years and only 13.6% of the respondents have been using tracking system for less than 5 years.

5.2 Verification of the Hypotheses

This section highlights a series of inferential analyses that were carried out to examine and establish the relationships between the different variables. The study used correlation analysis and regression analysis to examine the strengths and direction of the relationships in the variables as presented below.

This section highlights a series of inferential analyses that were carried out to examine and establish the relationships between the different variables. The study used correlation analysis and regression analysis to examine the strengths and direction of the relationships in the variables as presented below.

The correlation analysis was undertaken to examine the strength and direction of the relationships between the independent and dependent variables as explained in Table 4 below.

Table 4: Correlation analysis

Correlations		
		Effectiveness of the designed framework of data in motion
Consent	Pearson Correlation	.686 **
	Sig. (1-tailed)	.000
	N	44
		Effectiveness of the designed framework of data in motion
Confidentiality	Pearson Correlation	.342**
	Sig. (1-tailed)	.002
	N	44
		Effectiveness of the designed framework of data in motion
Privacy	Pearson Correlation	.589 **
	Sig. (1-tailed)	.000
	N	44

**. Correlation is significant at the 0.01 level (2-tailed).

Results in the Table 4 above reveal a significant relationship between consent and the effectiveness of the designed framework of data in motion. The correlation coefficient of .686 (**) with a significance value of .000 explain the nature of the relationship in this situation. This implies that seeking consent enhance trust and honesty, and empower the users to have the final say onwho retrieves their data unlike before when the service provider and other third parties wouldwithout seeking permission from the client.

The correlation results in the table above indicate a significant effect of confidentiality on the effectiveness of the designed framework of data in motion. The obtained correlation co-efficiency of .342(**) with a significance value of .000, explains the positive nature of relationship that exists between the two variables. This implies that in that situation, anonymity

of the users will be protected for their safety and security; it shall build trust, protects reputation and prevents misuse of confidential data.

Study findings, revealed a significant effect of privacy on the effectiveness of the designed framework of data in motion. The correlation coefficient of .589(**) with a significance value of .000 explain the nature of the relationship between the privacy, and the effectiveness of the designed framework of data in motion. Since the p.value is 0.000 higher than 0.01 the relationship is significant. This implies that in privacy, there is respect for individuals reputation and movement, enhance trust and individuals has a reasonable desire to keep something private. It also noted that privacy enables individuals manage their reputations as well as maintaining appropriate social boundaries.

Multiple regression analysis was used to compute the variation shared by the variables. It was used to identify how much variation lies in the relationship between the efficiency and the designed framework of data inmotion, as presented in Table 5 and Table 6.

Table 5: Model summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.713[a]	.508	.488	.71577679

a. Predictors: (Constant), Consent, Confidentiality and Privacy

Source: Primary data, 2023

From the model summary in Table 5, the multiple regression coefficient R was evidenced by 0.713. However, the adjusted R^2 shows that the ethical issues accounts for 50.8% of the efficiency of designed framework of data in motion; implying that the efficiency of designed framework of data in motion can be explained by 50.8% of their ethical issues; and the remaining 49.2% variation in the efficiency of designed framework of data in motion is due to other factors that were not part of this study.

Table 6: Coefficients table

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	T	Sig.
1	(Constant)	3.913	.129		.000	.000
	Consent	.245	.137	.245	1.783	.001
	Confidentiality	.304	.137	.304	2.220	.031
	Privacy	.313	.137	.313	2.310	.042

a. Dependent Variable: Performance of LTIL

Source: Primary data, 2023

The coefficients table shows that specifically, consent accounts for 24.5% variation in the efficiency of designed framework of data in motion. Further, confidentiality accounts for 30.4% variation in the efficiency of designed framework of data in motion. Furthermore, privacy accounts for 31.3% variation in the efficiency of designed framework of data in motion. The findings revealed that confidentiality and privacy had the highest effect on the efficiency of designed framework of data in motion.

6.0 Conclusions and Recommendations

6.1 Conclusions

The study concluded that there is a significant relationship between consent and the effectiveness of the designed framework of data in motion (r=.686**); implying that seeking consent enhance trust and honesty, and empower the users to have the final say onwho retrieves their data unlike before when the service provider and other third parties would without seeking permission from the client. Consent from the client, shall it enhance confidentiality and privacy. The study also concluded that there is a significant effect of confidentiality on the effectiveness of the designed framework of data in motion (r=.342**). This implies that in that situation, anonymity of the users will be protected for their safety and security; it shall build trust, protects reputation and prevents misuse of confidential data. Study findings finally concluded that there is a significant effect of privacy on the effectiveness of the designed framework of data in motion (r=.589**). This implies that in privacy, there is respect for individuals reputation and movement, enhance trust and individuals has a reasonable desire to keep something private. It also noted that privacy

enables individuals manage their reputations as well as maintaining appropriate social boundaries. Confidentiality and privacy of data in motion can lead to avoidance of reputation risks as a result of data breaches.

6.2 Recommendations

The study recommended the need for defined security framework for data. There is need for building a data security plan, and this plan includes defining requirements that shall help safeguard data in motion, address possible situations that could result in breaches, and raise awareness among workers and partners. All the organization employees should be aware of the security risks that could expose the organization to fines and fees due to inadequate cyber-security procedures.

The study recommended the need to implement technologies and processes. Thus, implementing systems and processes that ensure the safe transfer of sensitive data is vital towards ensuring data leaks and data theft are minimized. Data encryption plays a vital role in this step, and organizations should integrate it into common business workflows. Encryption requirements should be based on the latest standards by only allowing secure protocols.

It is also recommended that organizations looking into safeguarding data in transit against inside or outside attackers like malware attacks or intrusions should implement network security solutions such as firewalls and network access controls. Data Loss Prevention (DLP) solutions usually address the threats data in motion faces from breaches and human error during its transit.

The study recommended that the government of Uganda should legislate or formulate institutional and legal framework that governs the proper use of tracking systems in motion to ensure privacy and human rights of the car drivers.

Lastly, the study recommended that further research is therefore needed in areas such ‘legal framework governing designed framework of data in motion in Uganda’.

REFERENCES

Abaho, E. (2017). *Advancing Transportation in Uganda with Automation, Connectivity and Intelligence.* Kampala: MUK (Dissertation)

William, A., Mirembe (PhD), D. D. P., & Nabaasa (PhD), D. E. (2022). Data Privacy Analysis on E-commerce Application. *International Journal of Technology and Management*, *7*(2), 1-29. Retrieved from https://www.utamu.ac.ug/ijotm/index.php/ijotm/article/view/105

Barecki, B. (2019). *How to Protect Data in Motion.* Confidentiality and Privacy of Data. 3rd edition. Los Angeles, Sage.

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564–585. https://doi.org/10.1016/J.JACCPUBPOL.2018.10.006

William, A., Mirembe (PhD), D., & Nabaasa (PhD), E. (2023). Reducing Misuse of Data in Motion through Surveillance of Logs. *International Journal of Technology and Management*, *8*(1), 1-10. Retrieved from http://utamu.ac.ug/ijotm/index.php/ijotm/article/view/108

Haber, M. J., & Rolls, D. (2020). Identity Attack Vectors. In *Identity Attack Vectors* (pp. 107–116). Apress. https://doi.or/978-1-4842-5165-2_10*Hadoop*. (n.d.).

Katushabe, B.W. (2021). *Benefits of GPS Tracking Devices for Personal Vehicles*. Kampala. (KIU Dissertation). Unpublished.

Kagita, M. K., Thilakarathne, N., Rajput, D. S., & Lanka, D. S. (2020). *A Detail Study of Security and Privacy issues of Internet of Things*. http://arxiv.org/abs/2009.06341

Krejcie, R.V. & Morgan, D.W. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement.*

Lu, Y., & Xu, L. Da. (2019). Internet of things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103–2115. https://doi.org/10.1109/JIOT.2018.2869847

Manickam, P., Shankar, K., Perumal, E., Ilayaraja, M., & Kumar, K. S. (2019). Secure data transmission through reliable vehicles in vanet using optimal lightweight cryptography. In *Advanced Sciences and Technologies for Security Applications*. Springer. https://doi.org/10.1007/978-3-030-16837-7_9

Mukasa, D. (2021). *A GPS Tracker on Every 'Boda Boda':* A Tale of Mass Surveillance in Uganda. Kampala. Unwanted Witnesses.

Oppitz, M., & Tomsu, P. (2018). Security and Privacy Challenges. In *Inventing the Cloud Century* (Vol. 6, Issue 1, pp. 377–410). https://doi.org/10.1007/978-3-319-61161-7_14

Wlosinski, L. G. (2018). Data Loss Prevention — Next Steps. *ISACA Journal*, *1*, 1–11. https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2018/volume-1/data-loss-prevention-next-steps_joa_eng_0218