engineering proceedings

MDPI

Proceeding Paper

Examining Techniques to Enhance the Security and Privacy of IoT Devices and Networks against Cyber Threats †

Imran Qureshi [1,*], Mohammed Abdul Habeeb [1], Syed Ghouse Mohiuddin Shadab [1], Burhanuddin Mohammad [1], Mohammed Irfan [1], Syed Muhammad Shavalliuddin [1] and Mohit Gupta [2]

[1] College of Computing and Information Sciences, Department of IT, UTAS, Al Musannah, Muscat P. O. Box 74, Oman; habeeb@act.edu.om (M.A.H.); shadab@act.edu.om (S.G.M.S.); burhanuddin@act.edu.om (B.M.); mohammed.irfan@act.edu.om (M.I.); syed@act.edu.om (S.M.S.)
[2] Department of Civil Engineering, School of Engineering and Technology, Monad University, Hapur 245304, India; civilengineeringelearning@gmail.com
* Correspondence: imran@act.edu.om
† Presented at the 2nd Computing Congress 2023, Chennai, India, 28–29 December 2023.

Abstract: Improvements in technology have led to further enhancements in cyber security threats. Additionally, the mass application of IoT technology and networks has made the ecosystem vulnerable to cyber-attacks. Thus, this study focuses on analysing methods to enhance the security and privacy of IoT devices and networks against cyber threats/AI through a primary quantitative method. The methodology section looks into different factors associated with the development of the study. In order to analyse cyber security, a primary quantitative method is employed. It is found that factors such as data security protocol, type of IoT device, users' precautions, and regulatory policy are related to the security measures of the study. The discussion section briefly considers the findings of the study. Moreover, detailed observation can be found in the discussion section of the study.

Keywords: IoT devices; network security; data encryption; data security; cyber-attack protection; cyber security

Citation: Qureshi, I.; Habeeb, M.A.; Shadab, S.G.M.; Mohammad, B.; Irfan, M.; Shavalliuddin, S.M.; Gupta, M. Examining Techniques to Enhance the Security and Privacy of IoT Devices and Networks against Cyber Threats. *Eng. Proc.* **2024**, *62*, 23. https://doi.org/10.3390/engproc2024062023

Academic Editors: Geetha Ganesan, Xiaochun Cheng and Valentina Emilia Balas

Published: 15 April 2024

1. Introduction

The development of different technologies presents various associated risks. Ref. [1] there has been an 18% increase in weekly cyber attacks in India. Therefore, this study is focused on analysing methods that aid in enhancing the security and privacy of IoT devices and networks.

Data are considered among the major elements for the development of reliable IoT systems and networks. Therefore, securing data and databases is the primary challenge in ensuring the security of the network [2]. Additionally, anonymity in this process leaves a gap in the overall regulation process.

The Figure 1 conveys the global share of IoT attacks from 2019 to 2021.

It can be seen that there has been a drastic increase in cyber attacks since the third quarter of 2019 when global cyber attacks rose by 6%. At the same time, it was noticed that in the first quarter of 2021, the attacks increased by 19% [2]. Therefore, it can be stated that the security aspect of IoT devices and networks is volatile, and threats are evolving drastically. Hence, the nature of the threats and volatility justified the motive of this study.

1.1. Aim

The study aims to analyse methods to enhance the security and privacy of IoT devices and networks against cyber threats through a primary quantitative method.

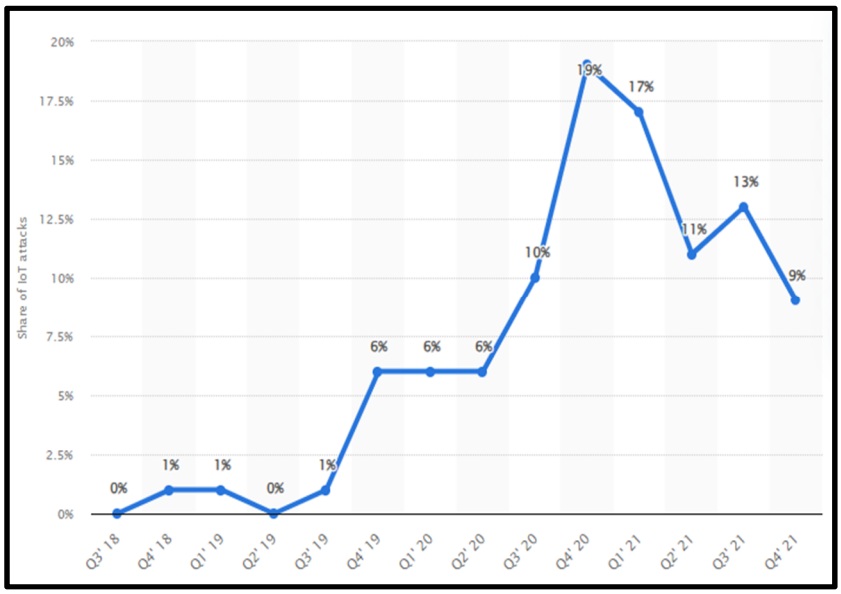

Figure 1. Global share of IoT attacks [2].

Research objective

RO 1: To analyse the factors associated with the security of IoT devices and networks.
RO 2: To analyse the role of regulatory policy in order to provide security of IoT devices and networks.
RO 3: To examine the role of users and user precautions training for securing IoT devices and networks.
RO 4: To elaborate on the challenges that are hindering the security of IoT and network security.

1.2. Research Question

RQ 1: What are the factors associated with the security of IoT devices and networks?
RQ 2: How does regulatory policy provide security for IoT devices and networks?
RQ 3: What is the role of users and user precautions training for securing IoT devices and networks?
RQ 4: What are the challenges, hindering the security of IoT and network security?

2. Literature Review

Factors Associated with the Security of IoT Devices and Networks

During the past literature analysis, it was noted that there are different components associated with the security of IoT devices and networks. As per the findings [3], the firmware of an IoT device and the operational network of a device is essential for providing security to the network. Moreover, updated firmware reduces risk by rectifying the gaps in previous firmware. On the other hand, ref. [4] argued that having an encrypted data transfer acts as a major factor in enhancing the security of the data. Additionally, using an encrypted form of data ensures data security by keeping the data available to both the sender and user [5]. Therefore, from the above discussion, it can be concluded that dating firmware and having encryption in devices act as a strong defence system against cyber attacks. Additionally, by using this primary defence system, the breaching of devices can be hindered.

Figure 2 displays the architecture of an IoT device that provides device-level security. As per the findings of [6], there is a continual risk of cyber assaults since IoT devices are manufactured in an unorthodox way and manage enormous amounts of data. Moreover, IoT device security and network security are among the broader factors that have different components. On the other hand, ref. [7] argued that ensuring network security works

as a primary level of defence for IoT devices and other devices. Therefore, incorporating components such as actuators and actuator analytics provides an understanding of the threats.

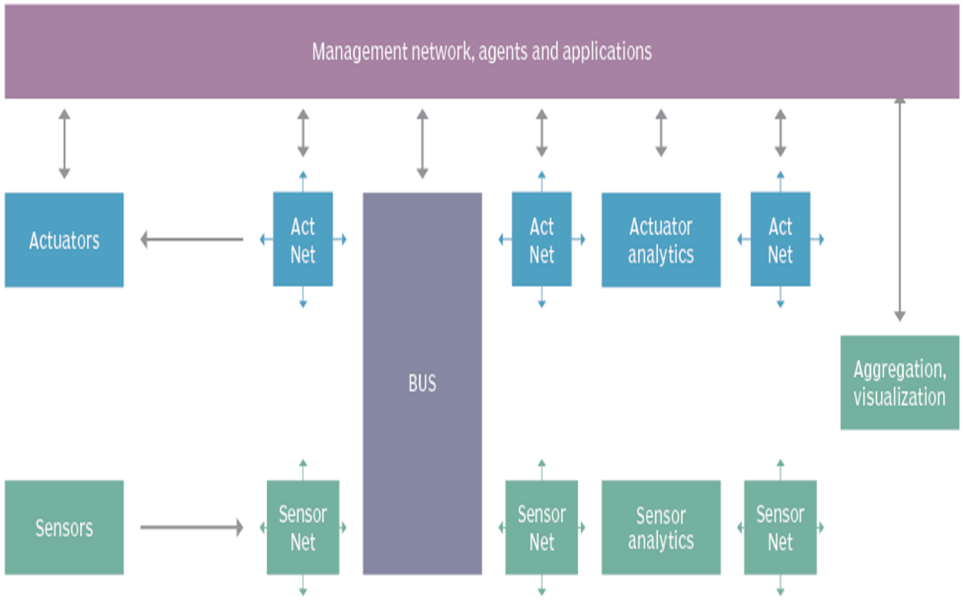

Figure 2. Components of IoT devices for the security of the device [7].

Figure 3 displays the different factors to be considered when analysing cyber security for IoT devices and networks. It was noticed that there are certain lays of cyber security that need to be considered. As per the findings of [8], network and IoT security is a volatile topic; thus, adjusting policy according to demand is important. Moreover, cyber security policies need to cover all possible components that could be detrimental in the future. On the other hand, ref. [8] argued that consistent monitoring needs to be integrated into policymaking in order to safeguard the interests of organisations and users. Moreover, through constant monitoring, it is possible to determine the risk factors. Thus, from the aforementioned discussion, it can be stated that policies need to be created based on the challenges of security. Additionally, constant monitoring of the data is essential.

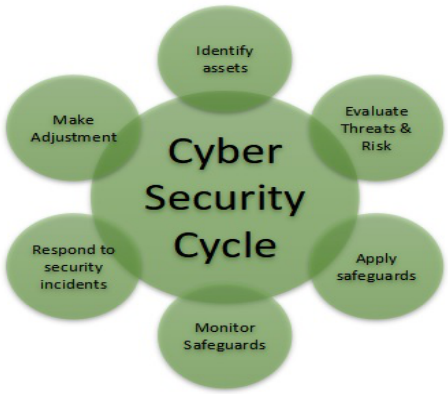

Figure 3. Factors of cyber security [8].

3. Methodology

3.1. Data Collection

The collection of data is one of the essential aspects of an empirical analysis. Therefore, primary sources of data were considered in order to analyse different factors associated with cyber security [9]. Primary sources of data allow for the collection of real-time

information for the accurate development of the study. In order to collect data for the study, a sample size of 75 respondents was surveyed. For the survey, a questionnaire comprising 13 questions was created. Out of the 13 questions, 10 were related to the chosen variable for the study. Additionally, 10 questions were related to the demographics of the participants [10]. Incorporating demographic analysis in a quantitative study aids in determining the impact of demographics on the answers of the participants. Additionally, the collection of real-time data allows one to develop a perspective related to the changes in a topic. Cyber security is a volatile topic; therefore, primary data sources were chosen in order to comprehend the real-time repercussions.

3.2. Data Analysis

After the collection of data, the method of analysis was chosen, which impacted the results of the study. Therefore, for the development of results based on the objectives of the study, quantitative methods of analysis were employed [10]. Quantitative methods of analysis help to establish relations among the different factors of an analysis. Thus, it is easier to contemplate the impact of independent variables on the dependent variable. IBM SPSS software was used in order to analyse the collected data. Additionally, regression analysis along with the coefficient, ANOVA, and the model summary table were integrated into the study [11]. Regression analysis aids in comprehending the significance of the factor along with the tendency. Moreover, any change in an independent variable and its impact on the dependent variable can be contemplated. A descriptive statistics table was incorporated in the study in order to contemplate the role nature of the data set.

Findings

Figure 4 displays the gender of the participants; the percentage of respondents can be analysed.

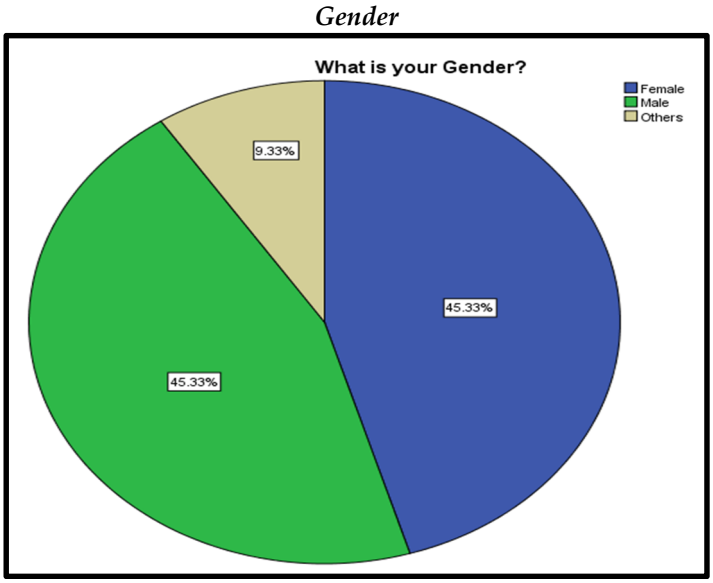

Figure 4. Pie chart associated with the gender of participants.

It can be seen that male participants represent 45.33% of the overall response. Similarly, female candidates have 45.33% representation according to the above image. Furthermore, 9.33% of candidates identified themselves as belonging to other gender categories.

Table 1 displays the gender statistics of the participants. The frequency of the respondents can be analysed from the data in the table. It can be seen that male candidates make up 34 out of 75 responses. Additionally, it can be seen that female candidates also make up 34 responses. However, there were 7 candidates who identified themselves as belonging to

other gender categories. Moreover, it can be stated that the population was well distributed based on the gender of the participants.

Table 1. The table associated with the gender of participants.

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Female	34	45.3	45.3	45.3
Male	34	45.3	45.3	90.7
Others	7	9.3	9.3	100.0
Total	75	100	100	

Figure 5 displays the age of the respondents; the percentage of participants can be analysed. It could be seen that participants below the age of 20 made up 21.33% of the overall sample population. Participants ranging between 20 and 35 years of age represented 41.33% of the overall sample population. Additionally, participants between the ages of 35 and 60 represented 37.33% of the sample population.

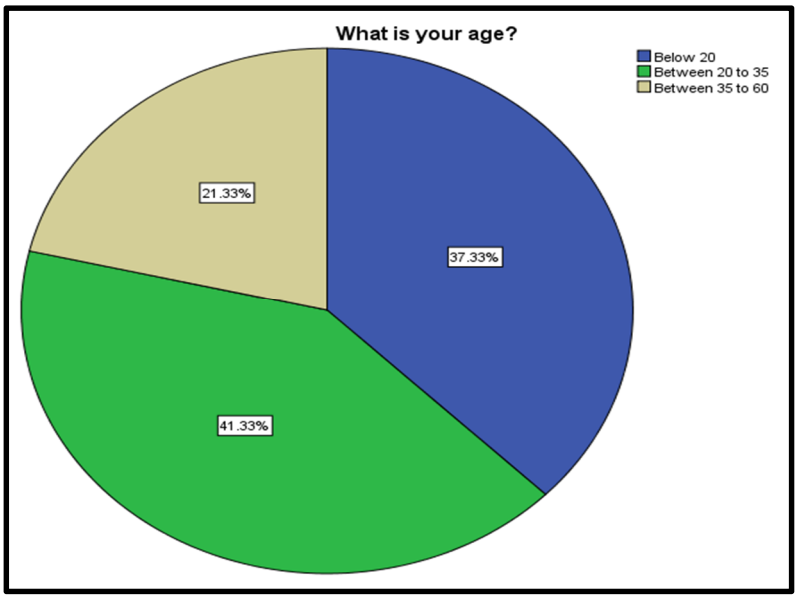

Figure 5. Pie chart related to age.

Table 2 displays the age-related statistics of other participants. The frequency of the respondent's age can be concluded from the above table. It can be seen that the frequency of respondents below the age of 20 is 28, and the frequency of respondents between 20 and 35 years of age is 31. Additionally, the group aged between 35 and 60 years had a frequency of 16 out of 75. Thus, it can be stated that the middle age group aged between 20 and 35 years represents the majority of the sample population.

Table 2. Table of age.

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Below 20	34	45.3	45.3	45.3
Between 20 and 25	34	45.3	45.3	90.7
Between 35 and 60	7	9.3	9.3	100.0
Total	75	100	100	

Figure 6 is associated with the income range of the respondents. It can be seen that respondents earning between RS 18,000 and 30,000 represented 46.7% of the overall population. Participants earning in the range of RS 30,000–50,000 represented 44% of

the overall population. Additionally, participants who were earning below RS 18,000 represented 9.3% of the overall population. However, there were no participants who were earning above RS 50,000.

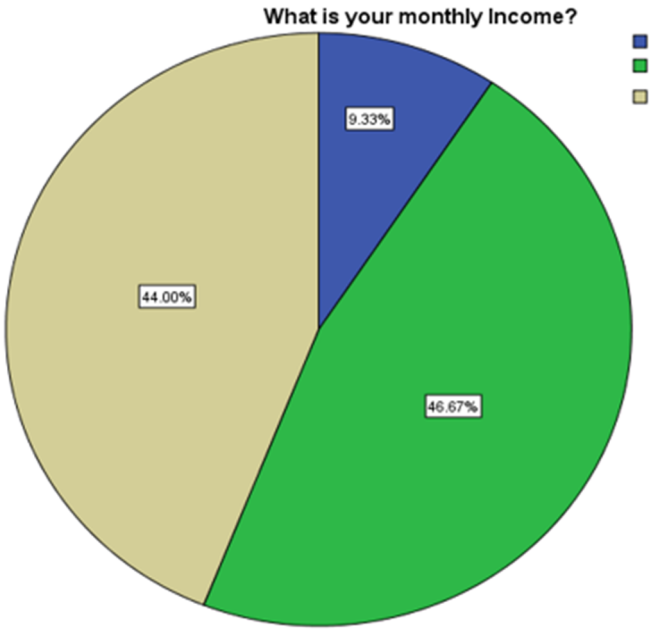

Figure 6. Pie chart related to income.

Figure 6 represents the income group out of which the blue colour shows income below Rs. 18,000, the green colour shows income between 18,000 and 30,000 and the remaining colour shows income between 30,000 to 50,000. Table 3 displays income-related information about the respondents. It can be seen that the participants earning below RS 18,000 had a frequency of 7 out of 75. Additionally, participants earning between RS 18,000 and 30,000 had a frequency of 35. Participants earning between RS 30,000 and 50,000 had a frequency of 33 out of 75. Hence, it can be stated that the population is well distributed according to the income range of the respondents.

Table 3. Table of income.

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Below RS 18,000	7	9.3	9.3	9.3
Between RS 18,000 and 30,000	35	46.7	46.7	46.7
Between RS 30,000 and 50,000	33	44.0	44.0	100.0
Total	75	100	100	

Table 4 displays the descriptive statistics of the variables. Descriptive statistics show the relationship and distribution of several variables. Ref. [11] shows that the mean and standard deviation values of the descriptive statistics may also be used to consider how the responses are clustered. To analyse the cyber security of IoT and networks, the security of IoT devices was chosen as the dependent variable of the study. The dependent variable showed a mean value of 3.6133 and a standard deviation value of 1.46022. Thus, it can be seen that the mean value is greater than the standard deviation.

Table 4. Descriptive statistics.

Descriptive Statistics												
	N	**Range**	**Minimum**	**Maximum**	**Mean**		**Std Deviation**	**Variance**	**Skewness**		**Kurtosis**	
	Statistic	**Statistic**	**Statistic**	**Statistic**	**Statistic**	**Std. Error**	**Statistic**	**Statistic**	**Statistic**	**Std. Error**	**Statistic**	**Std. Error**
DV	75	5.00	3.00	8.00	3.6133	0.16861	1.46022	2.132	2.579	0.277	5.256	0.548
IV1	75	6.00	2.00	8.00	3.7467	0.20008	1.73278	3.003	1.236	0.277	0.949	0.548
IV2	75	5.00	2.00	7.00	3.5467	0.18138	1.5079	2.467	1.137	0.277	0.151	0.548
IV3	75	5.00	3.00	8.00	4.0267	0.17499	1.51545	2.297	1.629	0.277	1.892	0.548
IV4	75	5.00	3.00	8.00	3.8267	0.19207	1.66338	2.767	1.713	0.277	1.376	0.548
Valid N (List wise)	75											

The first independent variable of the data security protocol provided a mean value of 3.7467 and a standard deviation value of 1.73278. For the second independent variable of the type of IoT device, the menace value was calculated to be 3.5467 and the standard deviation value was 1.57079. For the analysis, user precautions were chosen as the third independent variable and provided a mean value of 4.0267 and a standard deviation value of 1.51545.

Additionally, a regulatory policy was chosen as the fourth independent variable, with a mean value of 3.8267 and a standard deviation value of 1.66338 [11]. When the mean value is higher than the standard deviation value, answers are clustered around the mean. Additionally, the link between the mean value and the standard deviation value allows for the consideration of the data's distribution [12]. Thus, it can be contemplated that for all the variables, the responses were clustered around the mean value. Additionally, from a higher mean value it can be inferred that the speed of the data is not on the higher side. Hence, most of the participants agreed with the statements incorporated in the survey.

3.3. Regression Analysis

Hypothesis 1: *There is a relation between the security of IoT devices and the use of data security protocol*.

Table 5 displays the regression statistics of the first hypothesis of the study where different values of regression can be seen [13]. The significance value, when lower than 0.05, indicates that the hypothesis is supported with sufficient evidence. It can be seen that, for the first hypothesis, the significance value is 0.000, which is lower than 0.05. Thus, it can be stated that the first hypothesis is supported by sufficient evidence. Additionally, a significance value of 0.000 indicates that all the possible null hypotheses for the first hypothesis can be rejected [14]. Therefore, it can be stated that the use of data security protocols can enhance the security of IoT devices.

Additionally, R and R-squared change values are presented in the study [15]. With the interpretation of R and R-squared change values, the occurrence of impact can be contemplated. As per the coefficient table, the R-value for the first hypothesis is 0.692 and the R-squared change value is 0.479. Thus, it can be contemplated that a 69% change in the first independent variable of the data security protocol can impact the security of IoT devices [16]. Additionally, there is a 47% chance of such an occurrence. Therefore, it can be stated that data security protocols are important for enhancing the security of IoT devices and networks.

Table 5. Regression statistics of Hypothesis 1.

Model Summary											ANOVA						Coefficients										
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin Watson	Model	Sum of Squares	df	Mean Square	F	sig	Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig	Correlations			Collinearity Statistics	
					R Square Change	F Change	d1	df2	Sig. F Change									B	Std Error	Beta			Zero Order	Partial	Part	Tolerance	VIF
1	0.692	0.479	0.472	1.06069	0.479	67.247	1	73	0.000	2.276	Regression Residual total	75.657	1 73 74	75.657 1.125	67.247	0.000	1 (constant) IV1	1.427 0.584	0.293 0.071	0.692	4.864 8.200	0.000 0.000	0.692	0.692	0.692	1.000	1.000

Table 6. Regression statistics of Hypothesis 2.

Model Summary										Durbin Watson	ANOVA						Coefficients										
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics						Model	Sum of Squares	df	Mean Square	F	sig	Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig	Correlations			Collinearity Statistics	
					R Square Change	F Change	d1	df2	Sig. F Change									B	Std Error	Beta			Zero Order	Partial	Part	Tolerance	VIF
1	0.741	0.550	0.544	0.98647	0.550	89.143	1	73	0.000	2.633	Regression Residual total	86.784 71.038 157.787	1 73 74	86.784 0.973	89.143	0.000	1 (constant) IV2	1.169 0.689	0.283 0.073	0.741	40.132 9.442	0.000 0.000	0.741	0.741	0.741	1.000	1.000

Table 7. Regression statistics of Hypothesis 3.

Model Summary										ANOVA						Coefficients									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin Watson	Model	Sum of Squares	df	Mean Square	F	sig	Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig	Correlations			Collinearity Statistics	
					R Square Change	F Change	d1	df2	Sig. F Change									B	Std Error	Beta			Zero Order	Partial	Part	Tolerance	VIF
1	0.780	0.609	0.603	0.91951	0.609	113.621	1	73	0.000	2.805	1 Regression Residual total	96.066 61.721 157.787	1 73 74	96.066 0.845	113.621	0.000	1 (constant) IV2	0.586 0.752	0.303 0.071	0.780	1.932 10.659	0.057 0.000	0.780	0.780	0.780	1.000	1.000

Table 8. Regression statistics of Hypothesis 4.

Model Summary										ANOVA						Coefficients										
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin Watson	Model	Sum of Squares	df	Mean Square	F	sig	Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig	Correlations			Collinearity Statistics	
					R Square Change	F Change	d1	df2	Sig. F Change									B	Std Error	Beta			Zero Order	Partial	Part	Tolerance	VIF
1	0.762	0.581	0.575	0.95195	0.581	101.118	1	73	0.000	2.696	1 Regression Residual total	91.634 66.153 157.787	1 73 74	91.634 0.906	101.118	0.000	1 (constant) IV2	1.053 0.669	0.277 0.067	0.762	3.799 10.056	0.000 0.000	0.762	0.762	0.762	1.000	1.000

Hypothesis 2: *The type of IoT device and the system architecture plays a pivotal role in the security of IoT devices*.

Table 6 displays the regression analysis of the second hypothesis [17]. Device architecture is essential in order to provide a primary level of security. Additionally, the base security of the network initiates a strong data security protocol such as encryption. According to the regression analysis, the second variable provided a significance value of 0.000 which is lower than the base value of 0.05 thus, it can be stated that the second hypothesis is supported with sufficient evidence and the null hypothesis can be rejected. Moreover, the type of components has a major impact on enhancing the security of IoT devices.

Additionally, the second hypothesis provided an R-value of 0.741 and an R-squared value of 0.550 [17]. The R-value indicates the change and impact on the variables, and the R-squared value indicates the possibility of occurrence. Therefore, it can be stated that a 74% change in the second independent variable can impact the dependent variable of IoT devices and network security. Moreover, from the above analysis, it can be stated that the type of device and the device architecture are essential factors for enhancing the security of IoT devices and networks. Strong device security and protocols such as encryption programs ensure baseline security for IoT devices and networks.

Hypothesis 3: *Enhancement of security of IoT devices has a proportional relation with the user's precautions*.

Regression statistics of the third hypothesis are presented in Table 7. It can be seen that the regression analysis for the third hypothesis provided a significance value of 0.000. Therefore, as the significance value is lower than 0.05, it can be stated that the second hypothesis is supported with sufficient evidence. Moreover, users are one of the important aspects of the security of IoT and network security. Additionally, it can be seen that the F value for the third hypothesis is 113.62; thus, it is greater than 2.5 and the test is significant.

The R-value and R-squared change values of the third hypothesis are 0.780 and 0.609, respectively. Therefore, it can be stated that a 78% change in the third independent variable of user perception can impact the security of IoT devices and networks [18]. Additionally, there is a 60% chance of such an occurrence. Hence, it can be considered that training users in data security can drastically enhance security and reduce cyber-attacks.

Hypothesis 4: *Regulatory policy by a central body is directly related to the security of IoT devices*.

Regression analysis Hypothesis 4 is presented in Table 8 [19]. Regulatory policies play a pivotal role in the development of security measures for IoT and networks. Thus, regulation for security measures is considered the fourth independent variable for the study. It can be seen that the significance value for the fourth hypothesis is 0.000 which is lower than 0.05. Therefore, such a low significance value indicates that the fourth hypothesis is supported with sufficient evidence [20]. Additionally, a significance value of 0.000 indicates that the null hypothesis can be rejected for the fourth hypothesis.

At the same time, it can be seen that the R and R-squared change values for the fourth independent variable are 0.762 and 0.581, respectively. Based on the R and R-squared change values, it can be stated that a 76% change in the independent variable can impact the independent variable of IoT and network security. Additionally, there is a 58% chance of such an occurrence. Thus, it can be interpreted that the fourth independent variable is important for the security of the network and IoT devices. Additionally, by employing a central regulatory body for monitoring and preventing cyber attacks, it is possible to reduce the risk factors for IoT device use.

4. Discussion

Quantitative analysis was conducted in order to determine the factors for enhancing the IoT security and network security. For the study, primary data were considered and

analysed using quantitative methods. Moreover, a questionnaire with 10 variable-related questions and 3 demographic questions was considered for the study. The primary quantitative method of analysis aids in contemplating the relationship of the factors. Therefore, the primary quantitative method of analysis was chosen for analysing the volatile topic of enhancing security for IoT devices and networks. It was noted that the first hypothesis examining where the relation between the security of IoT devices and the use of data security protocol was considered to be was supported with sufficient evidence. Data security is the most important factor of network security [19].

Therefore, data security impacts network security. Furthermore, a second hypothesis indicated that the type of IoT device and the system architecture play pivotal roles in the security of IoT devices. A significance value of 0.000 was provided, indicating that there is enough evidence to support the second hypothesis. Furthermore, users play a pivotal role in the development of primary security measures for a network [19]. Thus, the third hypothesis indicated that the enhancement of security of IoT devices has a proportional relation with the user's precautions. The third hypothesis provided a significance value of 0.000, indicating the rejection of the null hypothesis.

Hence, it can be considered that training of users could be essential for the enhancement of security measures for IoT devices and network security. In the fourth hypothesis, regulatory policy by a central body was found to be related to the security of IoT devices and networks. The second hypothesis was found to be supported with sufficient evidence as the significance value was 0.000. Thus, a relevant perspective on security measures for IoT devices and networks can be drawn from the findings of the analysis.

5. Conclusions

A systemic analysis of the factors was conducted in order to develop a reliable study discussing the enhancement of security for IoT devices and networks. Factors such as data security protocol, type of IoT device, user precautions, and regulatory policy were analysed for the study. It was observed that there are certain factors such as users and device manufacturing that provide primary security for IoT devices and networks. Additionally, factors such as network architecture and regulatory measures are essential for ensuring the highest level of security. At the same time, the primary quantitative method of analysis aided in examining the relation between the different elements of network and IoT device security. Additionally, a coherent quantitative analysis was presented that provided reliable and tangible results for enhancing the security and privacy of IoT devices and networks.

Author Contributions: Conceptualization, I.Q.; methodology, I.Q.; software, I.Q, M.A.H.; validation, I.Q., M.A.H. and S.G.M.S.; formal analysis, B.M.; investigation, M.I., S.M.S.; resources, I.Q.; data curation, I.Q.; writing—original draft preparation, I.Q.; writing—I.Q, M.G.; visualization, M.I.; supervision, I.Q.; project administration, I.Q.; funding acquisition, I.Q.,All authors have read and agreed to the published version of the manuscript.

Funding: There is no funding available for this research.

Institutional Review Board Statement: Not Available.

Informed Consent Statement: Not Applicable.

Data Availability Statement: All the data itself available in the manuscript.

Conflicts of Interest: The authors declare no Conflict of interest.

References

1. Albaseer, A.; Abdallah, M. Privacy-Preserving Honeypot-Based Detector in Smart Grid Networks: A New Design for Quality-Assurance and Fair Incentives Federated Learning Framework. In Proceedings of the IEEE Consumer Communications and Networking Conference, CCNC, Las Vegas, NV, USA, 8–11 January 2023. [CrossRef]
2. Gupta, S.; Singh, G. An Empirical Study of IoT Technology to Enhance Data Breaches and Critical Protective Methods via Various Correlation. In Proceedings of the 2022 11th International Conference on System Modeling and Advancement in Research Trends, SMART 2022, Moradabad, India, 16–17 December 2022. [CrossRef]

3. Bocean, C.G.; Vărzaru, A.A. A Two-Stage SEM–Artificial Neural Network Analysis of Integrating Ethical and Quality Requirements in Accounting Digital Technologies. *Systems* **2022**, *10*, 121. [CrossRef]
4. Mohammed, H.; Hasan, S.R.; Awwad, F. Fusion-on-field security and privacy preservation for IoT edge devices: Concurrent defense against multiple types of hardware trojan attacks. *IEEE Access* **2020**, *8*, 36847–36862. [CrossRef]
5. Haghparast, M.B.; Berehlia, S.; Akbari, M.; Sayadi, A. Developing and evaluating a proposed health security framework in IoT using fuzzy analytic network process method. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 3121–3138. [CrossRef]
6. Fodor, M.; Viktor, P. IOT devices and 5G network security option from generation aspects. In Proceedings of the ICCC 2022-IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems, Proceedings, Reykjavík, Iceland, 6–9 July 2022. [CrossRef]
7. Ratkovic, N. Improving home security using blockchain. *Int. J. Comput. Inf. Manuf. (IJCIM)* **2022**, *2*, 27–37. [CrossRef]
8. Hassan, M.M.; Gumaei, A.; Huda, S.; Almogren, A. Increasing the Trustworthiness in the Industrial IoT Networks through a Reliable Cyberattack Detection Model. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6154–6162. [CrossRef]
9. Zhou, C.; Song, W.; Liu, L.; Niu, Z. Blockchain Technology-Enabled Smart Product-Service System Lifecycle Management: A Conceptual Framework. In Proceedings of the IEEE International Conference on Automation Science and Engineering, Hong Kong, China, 20–21 August 2020. [CrossRef]
10. Suhluli, S.A.; Khan, S.M.F.A. Determinants of user acceptance of wearable IoT devices. *Cogent Eng.* **2022**, *9*, 2087456. [CrossRef]
11. Chukwuere, J.E.; Molefe, B. The Impact of Data Security on the Internet of Things. In *Artificial Intelligence in Industry 4.0 and 5G Technology*; Chapter 5; Wiley: Hoboken, NJ, USA, 2022. [CrossRef]
12. Hamza, M.; Akbar, M.A.; Shafiq, M.; Kamal, T.; Baddour, A.M. Identification of Privacy and Security Risks of Internet of Things: An Empirical Investigation. *Rev. Comput. Eng. Res.* **2019**, *6*. Review of computer Engg Research. [CrossRef]
13. Alseady, S.; Baz, A.; Alsubait, T.; Alarabi, L.; Alhakami, H. Towards Security Challenges to Internet-of-Things: Big Data, Networks, and Applications. *Int. J. Comput. Sci. Netw. Secur.* **2020**, *20*, 131–141.
14. Ula, M.; Adek, R.T.; Mukhlish. Towards The Secure Internet of Things: Threats and Solution. In Proceedings of the Malikussaleh International Conference on Multidisciplinary Studies (MICoMS), Lhokseumawe, Indonesia, 30–31 January 2023; Volume 3. [CrossRef]
15. Khumalo, S.; Sibiya, A.; Teballo; Kekana, A. Strategies for Internet of Things Data Privacy and Security Using Systematic Review. In Proceedings of the European Conference on Information Warfare and Security, ECCWS, Chester, UK, 16–17 June 2022. [CrossRef]
16. Hussain, B.; Elmedany, W.; Sharif, M.S. The Internet of Things Security Issues and Countermeasures in Network Layer: A Systematic Literature Review. In Proceedings of the 2022 International Conference on Data Analytics for Business and Industry, ICDABI 2022, Sakhir, Bahrain, 25–26 October 2022. [CrossRef]
17. Chukwuere, J.E. Internet of Things (IoT) Cybersecurity Challenges and Mitigation Mechanisms. *Khazanah Sos.* **2022**, *4*, 235–240. [CrossRef]
18. Devarakonda, S.; Halgamuge, M.N.; Mohammad, A. Critical Issues in the Invasion of the Internet of Things (IoT): Security, Privacy, and Other Vulnerabilities. In *Research Anthology on Privatizing and Securing Data*; IGI Global: Hershey, PA, USA, 2021. [CrossRef]
19. Ali, A.; Mateen, A.; Hanan, A.; Amin, F. Advanced Security Framework for Internet of Things (IoT). *Technologies* **2022**, *10*, 60. [CrossRef]
20. Naria, I.P.; Sulistyo, S.; Widyawan. Security and Privacy Issue in Internet of Things, Smart Building System: A Review. In Proceedings of the 2022 International Symposium on Information Technology and Digital Innovation: Technology Innovation During Pandemic, ISITDI 2022, Padang, Indonesia, 27–28 July 2022. [CrossRef]