ISSN (e): 2250 – 3005 || Volume, 14 || Issue, 3|| May. - June. – 2024 ||
International Journal of Computational Engineering Research (IJCER)

Zero Trust Security and Multifactor Authentication in Fog Computing Environment

Varun Varma Sangaraju, *IEEE Member and Independent Researcher, USA*
SV Achuta Rao, *Professor & Dean, SreeDattha Institute of Engineering and Science, Hyderabad, India,*
Kathleen Hargiss, *Professor, University of the Cumberlands, KY, USA*

***Abstract*—*This quantitative correlational research study aimed to investigate the factors affecting the implementation of zero-trust security and multifactor authentication (MFA) in a fog computing environment. Fog computing is an emerging decentralized technology that extends cloud computing capabilities near the user. A fog computing environment helps in faster communication with the internet of things (IoT) devices and reduces data transmission overheads. However, the use of fog computing technology in information technology (IT) organizations is minimal in the United States. Many IT organizations lack trust in fog computing security, and these security issues can compromise high-priority systems within the network. Robust security mechanisms such as zero trust security and MFA are effective in non-perimeter-based systems such as the fog computing environment. This research study used the extended technology acceptance model (TAM) as the theoretical framework to evaluate the relationship between independent variables perceived usability, perceived ease of use, perceived security, perceived reliability, and dependent variable fog computing security adoption in IT. The study conducted a survey and collected samples from 125 IT professionals with experience in cloud/fog computing and zero-trust security. The study's results suggested that robust security mechanisms are necessary to use fog computing in the IT industry successfully.*

***Index Terms*—*fog computing, internet of things, multifactor authentication, quantitative methodology, technology acceptance model, zero trust security.*

Date of Submission: 27-04-2024 Date of acceptance: 05-05-2024

I. INTRODUCTION

THE importance of data in the 21st century has multiplied, and the information is stored in various forms. Data plays a crucial role in a human's day-to-day life. The rise of smartphones has allowed accessing data from anywhere globally through the internet. Data is considered valuable to an individual for personal reasons, for organizations to understand their customers, researchers, or scientists to create technology, and for governments to maintain countries. The need for the storage of large datasets and processing of the data was solved by cloud computing technology [1]. Unlike on-premises computing, organizations in the technology industry were provided with high computing resources on a pay-per-use basis in cloud computing [1]. However, the limitation of cloud computing is the connectivity between the internet of things (IoT) devices and the cloud computing environment due to vast geographical distribution [2][3]. A new layer is introduced between the user and the cloud computing environment, known as the fog computing environment. The fog computing paradigm is expected to be a cloud computing environment closer to the ground [3].

Fog computing is a decentralized system extending cloud computing capabilities where the data is processed near the edge devices to help in reducing data transmission overheads and faster communication with IoT

This paragraph of the first footnote will contain the date on which you submitted your paper for review, which is populated by IEEE. It is IEEE style to display support information, including sponsor and financial support acknowledgment, here and not in an acknowledgment section at the end of the article. For example, "This work was supported in part by the U.S. Department of Commerce under Grant 123456." The name of the corresponding author appears after the financial information, e.g. *(Corresponding author: Second B. Author).* Here you may also indicate if authors contributed equally or if there are co-first authors.
Varun Varma Sangaraju was with University of the Cumberlands, Williamsburg, KY, 40769 USA. (e-mail: varunvarma93@yahoo.com).
Kathleen Hargissis with University of the Cumberlands, Williamsburg, KY, 40769USA (e-mail: kathleen.hargiss@ucumberlands.edu).

devices [2][4][5]. The security of IoT applications is in jeopardy due to the lack of a reliable security mechanism in the fog computing environment [6]. Fog computing requires a robust security framework to safeguard IoT applications and the cloud computing environment. Zero trust security and MFA are among the security mechanisms that provide better security to IT systems. The zero-trust security model was first introduced by Kindervag in 2010 after analyzing the security shortcomings in the traditional perimeter-based model and suggesting that the insider cannot be trusted by default [7][8][9]. Multifactor authentication uses more than one form of authentication to verify the user [10].

II. BACKGROUND AND PROBLEM STATEMENT

The use of the internet and electronic devices such as smartphones, sensors, smartwatches, and fitness trackers has increased drastically [11]. The IoT is a connection of physical devices over a vast network with limited data processing power and storage [12]. The IoT is vital in many applications of smart homes, smart cities, and smart businesses [6]. The number of IoT devices connected to the internet may reach 500 billion by 2025 [6]. These IoT devices can process the data collected but do not have much processing power, and their resources are insufficient to host application services within themselves [5]. Usually, cloud computing systems collect vast amounts of data produced by IoT devices and process the information with their ability of high storage and computational power [12]. However, IoT applications that need quick turnaround responses and real-time analytics could not succeed due to the geographically distributed nature of cloud data centers [6].

Fog computing was proposed to support IoT devices that need location awareness and quick responses, but fog computing capabilities extend beyond IoT [3][11]. Fog computing can act as a bridge between the cloud computing environment and the IoT users to overcome specific bandwidth and processing time limitations [2][5][13][14]. Some latency-sensitive applications perform computing activities near the user with the help of fog computing [3]. Fog computing brings a wide array of applications by utilizing the limited availability of computing resources that were ineffective in cloud computing [15][16]. Fog computing has been adopted in various fields such as healthcare, smart cities, medical applications, mobile big data analytics, agriculture and farming, shopping centers, connected parking systems, and more [6][17]. As per the Open Fog Consortium (OFC) reports, the global fog computing market will reach $18.2 billion by 2022 [5].

Though fog computing has many benefits, the existing literature states that fog computing technology is hampering the security and privacy of IoT applications [6]. The amount of security and privacy standards for fog computing are negligible compared to cloud computing [6][18]. Some IT organizations lack trust in accepting fog computing technology due to the security concerns looming around it [6][19]. The fog computing technology calls for robust security mechanisms to safeguard the cloud computing environment and IoT applications.

Zero trust security is one of the robust security mechanisms implemented by many IT organizations such as Google, Microsoft, PagerDuty, Palo Alto, and Git Lab [20][21]. Zero-trust security considers every user trying to access the resources equally without trust and employs strict authentication and authorization mechanisms [7][8][22][23]. Zero trust security was implemented in mobile office applications helping organizations maintain better security outside of the network and in blockchain technology to improve user access management of the decentralized digital ledger system [7][24]. From the existing literature, it is learned that zero trust security can provide better security to decentralized networks such as blockchain and fog computing environments. Because fog computing networks are not a perimeter-defined technology, some security mechanisms like zero trust security are required.

Zero trust security depends on a solid authentication strategy such as MFA, and MFA compliments the existence of zero trust security [20][22][23]. The increase in compromised security instances in the digital era showcased that only one level of authentication does not secure the environment [25]. The use of more than one form of authentication is known as MFA [10][25], which significantly reduces online security breaches because the stolen passwords of the users alone are insufficient for the attackers to intrude on the system [26]. This motivated security professionals to implement multiple authentication mechanisms [10][27].

The fog computing environment is an extension of cloud computing and inherits most of the security concerns in the cloud computing environment [6]. As fog computing is a decentralized system, the fog nodes are distributed across the network, and the risk of securely managing all the nodes is high [6][16]. The fog nodes can leave or join the network at any time because they might be portable devices that move geographically, which multiplies the security risk [28][29]. The security of IoT applications is compromised due to accessing corrupted fog nodes [29]. Trust in the fog computing nodes is minimal among the technology industries to adopt this decentralized concept [19][30]. A robust security framework for the fog computing environment is not found in the existing body of knowledge.

A robust security framework is required to overcome some or most security concerns in the fog computing environment. Zero trust security is a framework in which every subject in the network is not implicitly trusted and will be verified for every transaction [22][23]. Though some trust mechanisms are proposed for fog computing, existing literature does not show evidence of zero trust security use in fog computing. Multifactor authentication is a security mechanism that enforces more than one form of authentication to verify the subject [22][23]. The number of security breaches was reduced using MFA, and the security experts were motivated to use it [10][27]. Multifactor authentication is an essential mechanism supporting zero trust security [20][22][23].

This quantitative study used TAM to understand the factors affecting the implementation of a zero-trust security framework and MFA in the fog computing environment. The population of this study was IT professionals with knowledge of distributed and decentralized systems. There was minimal to no research on using zero-trust security and multifactor authentication in fog computing networks, per the researcher's knowledge. The problem statement identified was the gap in existing literature where the fog computing environment is responsible for decreasing the security level of IoT applications, and the trust in a fog computing environment is low for acceptance in IT industries [6][19][30].

III. PURPOSE AND SIGNIFICANCE OF THE STUDY

The research problem adopted quantitative methodology and correlational research design to understand factors affecting the implementation of proposed security mechanisms, zero-trust security, and MFA in a fog computing environment through statistical models.The scope of this research was to understand whether the organizations are willing to adopt a fog computing environment after implementing security measures such as zero trust security and MFA. From the literature, it is evident that the fog computing environment degrades the security of IoT applications, and organizations cannot trust the technology for security reasons [6][19][30]. The researcher expects that the proposed security mechanisms could improve the overall security of fog computing, but the study must determine the outcome.

The population for this study was the IT professionals that have worked on projects consisting of centralized and decentralized mechanisms in the United States. The experience of these IT professionals, who have knowledge of technologies such as cloud computing, fog computing, edge computing, zero trust security, and MFA, allowed for the analysis of the research problem. This study was conducted through the QuestionPro audience database. Though no geographical restrictions were applied, all the participants were residents of the United States.

This study was one of the first to understand the factors related to adopting zero-trust security and MFA in a fog computing environment. The overall security problem in fog computing is known to researchers and IT organizations, and the organizations are not confidently implementing fog computing technology [6][19][30]. After extensive research, the researcher identified security mechanisms such as zero trust security and MFA that can mitigate the fog computing security problem. No prior studies indicated the successful implementation of all these technologies together. This study investigated the factors in implementing zero-trust security and MFA in a fog computing environment. This study was essential to understand the possibility of these security mechanisms in a fog computing environment and adopt these technologies in the IT industries. The results of this research could be a scale to measure the implementation of security mechanisms or algorithms in a fog computing environment. This study could provide future researchers with a scope to constantly improve the security of the fog computing environment.

IV. RESEARCH QUESTIONS

The primary research question evolved from the research problem: "What factors affect the implementation of zero trust security and MFA in a fog computing environment?" The researcher understood the importance of security in a fog computing environment and aimed to understand the factors affecting the use of zero trust security and MFA in a fog computing environment. This study was elaborated on to understand the relationship between the factors mentioned in the research question and the research problem:

RQ1: What is the relationship between perceived usefulness and implementation of zero trust security and MFA in a fog computing environment?

RQ2: What is the relationship between perceived ease of use and implementation of zero trust security and MFA in a fog computing environment?

RQ3: What is the relationship between perceived security and implementation of zero trust security and MFA in a fog computing environment?

RQ4: What is the relationship between perceived reliability and implementation of zero trust security and MFA in a fog computing environment?

These research questions supported understanding the factors holding the users from implementing zero-trust security and MFA in a fog computing environment.

The leaders of IT organizations must understand the expert opinions on new-age technologies like fog computing and zero-trust security before making necessary business decisions. This study was conducted to understand the reasons better for using zero trust security in a fog computing environment. Examining the correlation between the adoption of zero-trust security and MFA in a fog computing environment and various factors such as ease of use, usability, security, and reliability are discussed. The following section discusses the study's theoretical framework with necessary factors.

V. THEORETICAL FRAMEWORK AND INSTRUMENTATION

TABLE I
STUDY VARIABLES AND THEIROPERATIONAL DEFINITIONS

Variable Reference	Operational Definitions from Literature
Perceived Ease of Use (PEOU)	PEOU measures an individual's perception of the ease of use in adopting zero trust security and multifactor authentication in a fog computing environment on a Likert scale of 1-5 [31].
Perceived Usability (PU)	PU measures an individual's perception of usability in adopting zero trust security and multifactor authentication in a fog computing environment on a Likert scale of 1-5 [31].
Perceived Security (PS)	PS measures an individual's perception of the security of the systems in adopting zero trust security and multifactor authentication in a fog computing environment on a Likert scale of 1-5 [32].
Perceived Reliability (PR)	PR measures an individual's perception of the reliability of the systems in adopting zero trust security and multifactor authentication in a fog computing environment on a Likert scale of 1-5 [32].
Fog Computing Security Adoption in IT	Behavioral Intention (BI) measures an individual's perception of adopting zero trust security and multifactor authentication in a fog computing environment on a Likert scale of 1-5 [33].

The theoretical framework used for this study was an extended TAM, which is an established model to measure technology adoption with proven reliability and validity [32]. The use of the TAM model in IT is common, and researchers can add external variables if they prove beneficial to technology adoption [32][33]. Originally, PEOU and PU were the only variables present in TAM [31]. This research study added external variables such as perceived security and perceived reliability affecting technology adoption [32][33]. The TAM model was used for this study based on its flexibility in understanding external factors that can impact the technology adoption of the latest technologies, such as zero-trust security and MFA in a fog computing environment. The survey consists of 15 questions based on a 5-point Likert-type scale from 1 to 5. All the survey questions were statements followed by the 5-point scale representation as 1-Strongly Disagree, 2-Disagree, 3-Neutral, 4-Agree, and 5-Strongly Agree for measuring the user's perceptions of the technology. Four variables were identified for this study: perceived usefulness, perceived ease of use, perceived reliability, and perceived security. Table 1 mentions the study's variables and their operational definitions.

VI. RESEARCH FINDINGS

A. Participants and Research Setting

This study was a quantitative correlational research study to understand the relationship between the factors influencing the adoption of zero trust security and MFA in a fog computing environment. The population of this study was IT professionals with experience working in cloud computing/fog computing technology and zero-trust security in the United States. The population was obtained from an online survey platform called QuestionPro.

The G*Power model used for this study consisted of F-tests with Linear multiple regression: Fixed model, R^2 deviation from zero. A priori type of power analysis was used to determine the sample size. The parameters for this test are effect size f2 as 0.15, alpha error probability as 0.05, power as 0.90, and the number of predictors as four. The model returned the total sample size required for this study as 108, but a sample of 125 was acquired. The sample is collected from the members of the database called QuestionPro Audience. The participants were from various geographical regions within the United States. The participants of the sample selected 'Yes' as their consent after reading the informed consent form consisting of the details such as the researcher's information, institution details, and instructions required to complete the survey, including the approximate time taken to complete the survey. The participants were then taken to the inclusion/exclusion criteria page to understand their eligibility to participate in the survey. Eligible participants were administered the 15 survey questions. All 125 members who participated in the survey were deemed eligible to answer the survey questions.

Demographic information such as gender, job function, and the experience were collected for data analysis. Of 125 participants, 90 were male, constituting 72%, and 35 were female or 28%. The population required for this study was IT professionals working in the industry currently. The information regarding the participants' job functions was collected. Table 2 represents the details related to the IT job function of the participants. The participants' experience showcases their knowledge and understanding of the problem statement. The analysis of the experience data of the participants is presented in Table 3.

TABLE II

PARTICIPANT'S JOB FUNCTION IN IT

Job Function	**Frequency**	**Percent**	**Cumulative Percent**
Chief Executive Officer	6	4.8	4.8
Chief Technology Officer	8	6.4	11.2
Executive Member	3	2.4	13.6
IT Director	22	17.6	31.2
IT Manager	40	32.0	63.2
Other	20	16.0	79.2
Software Engineer	14	11.2	90.4
Supervisor	2	1.6	92.0
System Administrator	2	1.6	93.6
Vice President	8	6.4	100.0
Total	125	100.0	

TABLE III

PARTICIPANT'S EXPERIENCE IN IT

Experience	**Frequency**	**Percent**	**Cumulative Percent**
Chief Executive Officer	24	19.2	4.8
Chief Technology Officer	49	39.2	11.2
Executive Member	30	24.0	13.6
IT Director	14	11.2	31.2
IT Manager	5	4.0	63.2
Other	3	2.4	79.2
Total	125	100.0	

IBM SPSS (Version 28) and JASP (Version 0.16.2) were used to analyze the data acquired through this research study. The collected data was loaded into SPSS for data analysis and statistical tests. IBM SPSS was used to conduct a descriptive analysis of the participant's demographic information, tests of assumptions on the data to identify suitable statistical models, correlation of the variables, and hypothesis testing. Test of assumptions and reliability tests were conducted before the analysis of research questions so that appropriate statistical tests could be determined.

B. Test of Assumptions Results

The tests of assumptions were performed to evaluate the primary assumption of the multiple linear regression. An assumption is considered a condition that ensures that the researcher's attempt works [34]. A test of assumptions is necessary to understand if the assumed statistical tests are valid for the data collected [34]. If the assumptions are false, the statistical tests conducted based on the assumptions can lead to inaccurate conclusions [34]. The assumption tests used for this study were homoscedasticity, independent errors, tests of normality, and linearity.

A Normality test can be conducted using Shapiro-Wilk Test and a P-P plot. A P-P plot provides the cumulative probability of a variable against the cumulative probability of a particular distribution [34]. This study used a P-P plot to test the linear relationship between the independent and dependent variables. As per the P-P plot in Figure 1, there is some deviation in the data points from the linear. The normality test determined that the data was not normally distributed, and it was appropriate to perform non-parametric tests on the sample data.

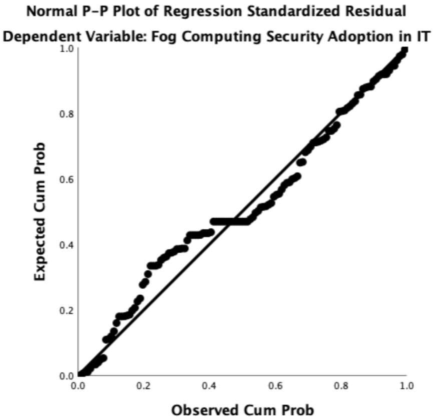

Fig. 1. P-P plot for Normality test

C. Reliability

This study consisted of 15 survey questions with a collected sample of 125. The survey instrument Dawson used in this study was tested for reliability and consistency, but the researcher modified it according to the problem statement [32]. Though the survey was well established, a reliability test must be conducted for the data citing various reasons such as survey modification aligning to the research problem, different sample size, and population from the original creator [34][35]. Cronbach's alpha is an internal consistency measure used to understand how closely the items in a set are related [33][34]. The survey instrument, with 125 participants answering 15 questions, achieved a Cronbach's alpha score of .946. The Cronbach's alpha score of more than .7 is considered an acceptable measure of consistency and reliability [34]. According to [36], Cronbach's Alpha value of >= .9 is considered excellent, >= .8 is considered good, >= .7 is considered acceptable, >= .6 is considered questionable, >= .5 is considered poor, and < .5 is considered unacceptable.

D. Bayesian Pearson's Correlation

Bayesian Pearson's Correlation (r) was used to determine the relationship between the independent and dependent variables of the study. According to [37], an r value greater than 0.5 denotes a strong correlation, an r value greater than .3 but lesser than .5 denotes moderate correlation, and an r value greater than .1 and lesser than .3 indicates little correlation.

Bayesian Pearson's correlation results indicates that perceived usefulness strongly correlates with other study variables, and the values are r = .765, r = .768, r = .742, and r = .672. Perceived ease of use strongly correlates with other study variables, and the values are r = .765, r = .801, r = .826, and r = .747. Perceived security strongly correlates with other study variables, and the values are r = .768, r = .801, r = .824, and r = .769. Perceived reliability strongly correlates with other study variables, and the values are r = .742, r = .826, r = .824, and r = .771. The dependent variable strongly correlates with other study variables, and the values are r = .672, r = .747, r = .769, and r = .771.

E. Analyses of Research Questions

A non-parametric test was conducted because the data proved not normally distributed. The research questions of this study were tested using the Bayesian regression model. The study's hypotheses determined the relationship between independent and dependent variables. Each hypothesis test was conducted using Bayesian linear regression analysis to evaluate and conclude whether to reject or fail to reject the null hypothesis. The Bayesian regression model for hypothesis testing was conducted through the JASP software.

While the p-values in traditional frequentist regression models can only confirm acceptance or rejection of a null hypothesis, the Bayesian regression hypothesis testing using Bayesian factors can state evidence for the acceptance of the alternative hypothesis [38]. Bayesian hypothesis testing provides rich information compared to p-values strengthening the credibility of an analysis [38][39]. When a Bayesian hypothesis test is conducted via Bayesian factor BF_{10}, H_1 is relative to H_0, and an alternative hypothesis can be accepted or rejected based on the results [38][39].

One of the assumptions of Bayesian regression tests is prior distributions. Bayesian regression has two types of prior distributions to be selected before running the models [40]. The first one is model prior, which is used to assign a prior probability to each model [40]. The model prior used in JASP for this research was beta-binomial with values of a = 1, b = 1. The second one is prior, which is used to assign a normal distribution to each regression coefficient [40]. The prior used in JASP for this research was Jeffreys-Zellner-Siow (JZS) with an r scale = 0.354. The values for both the prior distributions were default JASP values loaded by the software.

After running all the models necessary for this research, the prior was determined as an informative prior [41]. The informative priors contain numerical values, which are crucial to model estimation and leave a significant impact on final estimates [41].

1) **Research Question One**

This section presents the first research question of the study and appropriate statistical test results obtained by performing Bayesian linear regression.

RQ1: What is the relationship between perceived usefulness and implementation of zero trust security and multifactor authentication in a fog computing environment?

The first hypothesis is deduced from the first research question.

$H_0$1: There is no significant relationship between perceived usefulness and implementation of zero trust security and multifactor authentication in a fog computing environment.

H_a1: There is a significant relationship between perceived usefulness and implementation of zero trust security and multifactor authentication in a fog computing environment.

The results of testing Hypothesis One with Bayesian linear regression indicated that the Bayesian factor value for the alternative H_1 relative to H_0, BF_{10} = 4.150e+14 is non-zero and significantly larger than 1. As the values of BF_{10} from Table 4 for Perceived Usefulness are much larger than 1, the null hypothesis is rejected. Hence, the hypothesis suggested that there is a significant relationship between perceived usefulness and implementation of zero trust security and multifactor authentication in a fog computing environment.The R^2 value of 0.452 from Table 4 indicated that the independent variable accounted for 45.2% of the variance in the model.

TABLE IV
MODEL COMPARISON OF PERCEIVED EASE OF USE

Models	P(M)	P(M|data)	BF_M	BF_{10}	R²
Null model	0.500	2.410e-15	2.410e-15	1.000	0.000
Perceived Usefulness	0.500	1.000	4.094e+14	4.150e+14	0.452

2) **Research Question Two**

This section presents the second research question of the study and appropriate statistical test results obtained by performing Bayesian linear regression.

RQ2: What is the relationship between perceived ease of use and implementation of zero trust security and MFA in a fog computing environment?

The second hypothesis is deduced from the second research question.

$H_0$2: There is no significant relationship between perceived ease of use and implementation of zero trust security and MFA in a fog computing environment.

H_a2: There is a significant relationship between perceived ease of use and implementation of zero trust security and MFA in a fog computing environment.

The results of testing Hypothesis Two with Bayesian linear regression indicated that the Bayesian factor value for the alternative H_1 relative to H_0, BF_{10} = 1.788e+20 is non-zero and significantly larger than 1. As the values of BF_{10} from Table 5 for Perceived Ease of Use are much larger than 1, the null hypothesis is rejected. Hence, the hypothesis suggested that there is a significant relationship between perceived ease of use and implementation of zero trust security and MFA in a fog computing environment.The R^2 value of 0.558 from Table 5 indicated that the independent variable accounted for 55.8% of the variance in the model.

TABLE V
MODEL COMPARISON OF PERCEIVED EASE OF USE

Models	P(M)	P(M|data)	BF_M	BF_{10}	R²
Null model	0.500	5.592e-21	5.592e-21	1.000	0.000
PerceivedEaseofUse	0.500	1.000	∞	1.788e+20	0.558

3) **Research Question Three**

This section presents the third research question of the study and appropriate statistical test results obtained by performing Bayesian linear regression.

RQ3: What is the relationship between perceived security and implementation of zero trust security and multifactor authentication in a fog computing environment?

The third hypothesis is deduced from the third research question.

$H_0$3: There is no significant relationship between perceived security and implementation of zero trust security and multifactor authentication in a fog computing environment.

H_a3: There is a significant relationship between perceived security and implementation of zero trust security and multifactor authentication in a fog computing environment.

The results of testing Hypothesis Three with Bayesian linear regression indicated that the Bayesian factor value for the alternative H_1 relative to H_0, BF_{10} = 1.876e+22 is non-zero and significantly larger than 1. As the values of BF_{10} from Table 8 for perceived security are much larger than 1, the null hypothesis is rejected. Hence, the hypothesis suggested that there is a significant relationship between perceived security and implementation of zero trust security and multifactor authentication in a fog computing environment.The R^2 value of 0.591 from Table 6 indicated that the independent variable accounted for 59.1% of the variance in the model.

TABLE VI

MODEL COMPARISON OF PERCEIVED SECURITY

Models	P(M)	P(M|data)	BF_M	BF_{10}	R^2
Null model	0.500	5.329e-23	5.329e-23	1.000	0.000
Perceived Security	0.500	1.000	∞	1.876e+22	0.591

4) **Research Question Four**

This section presents the fourth research question of the study and appropriate statistical test results obtained by performing Bayesian linear regression.

RQ4: What is the relationship between perceived reliability and implementation of zero trust security and multifactor authentication in a fog computing environment?

The fourth hypothesis is deduced from the fourth research question.

$H_0$4: There is no significant relationship between perceived reliability and implementation of zero trust security and multifactor authentication in a fog computing environment.

H_a4: There is a significant relationship between perceived reliability and implementation of zero trust security and multifactor authentication in a fog computing environment.

The results of testing Hypothesis Four with Bayesian linear regression indicated that the Bayesian factor value for the alternative H_1 relative to H_0, BF_{10}= 3.429e+22 is non-zero and significantly larger than 1. As the values of BF_{10} from Table 7 for perceived reliability are much larger than 1, the null hypothesis is rejected. Hence, the hypothesis suggested that there is a significant relationship between perceived reliability and implementation of zero trust security and MFA in a fog computing environment.The R^2 value of 0.595 from Table 7 indicated that the independent variable accounted for 59.5% of the variance in the model.

TABLE VII

MODEL COMPARISON OF PERCEIVED RELIABILITY

Models	P(M)	P(M|data)	BF_M	BF_{10}	R^2
Null model	0.500	2.916e-23	2.916e-23	1.000	0.000
Perceived Reliability	0.500	1.000	∞	3.429e+22	0.595

F. Practical Assessment of Research Questions

Research Question One and Hypothesis One examined the impact of perceived usefulness and implementation of zero trust security and MFA in a fog computing environment. This independent variable suggested that perceived usefulness is a strong indicator in one's opinion to adopt new security mechanisms in a fog computing environment.The respondents agreed with the impact of perceived usefulness on this research study. For example, 90.4% of the respondents have agreed or strongly agreed that security mechanisms such as zero trust security and MFA in a fog computing environment would be useful in the IT industry. Only 5.6% disagreed or strongly disagreed when asked if this technology would make their job easier. Most IT professionals in the United States believed that robust security mechanisms in a fog computing environment would be useful in their work environment and improve their job performance. Additionally, IT organizations need to understand how their employees perceive the usefulness of new security mechanisms in a fog computing environment and adapt in everyone's best interests.

Research Question Two investigated the impact of perceived ease of use and implementation of zero trust security and MFA in a fog computing environment. The results of the hypothesis test indicated that the perceived ease of use had a significant impact on the adoption of new security methods in the fog computing environment in the IT industry.The participants of this study had high levels of perceived ease of use. For example, only 3.4% of the respondents disagreed or strongly disagreed when asked if it is easy to become skillful at using zero trust security and MFA in a fog computing environment. Similarly, only 4% asserted that learning to operate zero trust security and MFA in a fog computing environment would not be easy. Among all respondents, 86.4% agreed or strongly agreed that interacting with zero trust security and MFA in a fog computing environment would be clear and understandable for them. Information technology professionals in the United States believed that using zero trust security and MFA in a fog computing environment would be easy to use, learn, and navigate. More IT organizations must provide appropriate training for their staff to use the technology effectively.

Research Question Three examined the impact of perceived security and implementation of zero trust security and MFA in a fog computing environment. The results of the hypothesis test indicated that perceived security had a significant impact on the adoption of new security methods in the fog computing environment in the IT industry. This independent variable suggested that perceived security is a strong indicator in one's opinion to adopt new security mechanisms in a fog computing environment. Prior studies indicated that security of fog computing environment is vulnerable and IT industry exhibited lower trust [6][19][42]. However, the results of perceived security indicated that the use of robust security mechanisms in fog computing environment can change the security perceptions of IT professionals.The respondents agreed with the positive impact of perceived security on this research study. After looking into the insights, 97.6% of the respondents felt that zero trust security and MFA in a fog computing environment are secure. Only 3.2% of the respondents felt that zero trust security and MFA in a fog computing environment are not more secure than traditional security methods. Of the participants, 98.4% did not have any problems recommending zero trust security and MFA in a fog computing environment as a secure technology in their organization. The IT professionals in the United States believed that zero trust security and MFA were more secure methods to use in a fog computing environment than traditional methods and would be comfortable recommending them to their organization. More IT organizations must collect feedback from their security specialists and subject matter experts to make the fog computing environment secure.

Research Question Four examined the impact of perceived reliability and implementation of zero trust security and MFA in a fog computing environment. The results of the hypothesis test indicated that perceived reliability had a significant impact on the adoption of new security methods in the fog computing environment in the IT industry.The participants of this study had high levels of perceived reliability. From the data analysis, only 4% of the respondents feel that zero trust security and MFA in a fog computing environment are not more reliable than traditional security methods. Supporting the evidence, only 4% of the respondents would not feel comfortable recommending zero trust security and MFA in a fog computing environment to their organization. The IT professionals in the United States felt that zero trust security and MFA were more reliable security mechanisms to use in a fog computing environment than traditional security methods and would be comfortable recommending them to their organization. More IT organizations must consider security seriously and provide reliable IT systems for their employees to work.

VII. IMPLICATIONS FOR FUTURE STUDY

The security of IT systems is of great importance to organizations. One faulty system can corrupt all the other good systems. Security is one of the significant problems for the existence of fog computing in the IT enterprise. The respondents of this study suggested that zero-trust security and MFA in a fog computing environment were more secure than traditional security methods, and they felt comfortable recommending them to their organization. They also felt that the proposed security system of fog computing was more reliable than the traditional security methods. IT organizations must consult with the subject matter experts of the systems and the security advisors or specialists of the organization. System Architects, IT managers, security specialists, and business analysts must be involved in the design of zero trust security and MFA in the fog computing environment. Every system is different in an IT organization and embedding new technology takes enormous planning and effort. Organizations must provide appropriate training to all the IT systems staff because security breaches can happen in the form of one under-trained user. When IT organizations address the security of fog computing systems through zero-trust security and MFA, IoT devices will have more advantages, and the technology will become available to the public.

The results of this research study provide a foundation for future fog computing security research. This research study was conducted with a sample in the United States of America. The scope of future research can be extended to other countries to determine the factors affecting the implementation of zero trust security and MFA in fog computing environments globally. The research was conducted on IT professionals with experience in fog computing and zero trust security. The future scope of the research can be in new domains such as technology institutions, business customers, and the public at some point. The sample for this study was collected from the QuestionPro audience database. The data sample for future studies can be collected through different mediums to observe any variances compared to this research study.

The study results showed that implementing zero trust security and MFA in a fog computing environment would be beneficial in many ways. This research study evaluated four pre-defined constructs of the extended TAM model. Future research can try to understand more factors that can impact the implementation of fog computing security. The fog computing environment applied in this research is a generalized concept. However, there is a scope to apply specific devices related to IoT to fog computing security. Finally, the study was conducted as a quantitative and correlational research study. Nevertheless, there is a scope to conduct the research in qualitative methodology to collect more detailed information from the participants and interpret the results differently.

VIII. CONCLUSION

The purpose of this quantitative correlational research study was to investigate the factors affecting the implementation of zero trust security and MFA in a fog computing environment. A sample size of 125 was collected from the QuestionPro audience database in the United States to analyze four independent variables, which were perceived usability, perceived ease of use, perceived security, and perceived reliability. The extended TAM model was the foundational framework for this research study adopted from [32], and the results showed that all the variables are statistically significant when computed against the dependent variable. The null hypothesis was rejected, and all four alternate hypotheses were accepted.

This research adds to the existing body of knowledge by showcasing the factors affecting the implementation of robust fog computing security. The primary outcome of this study is that the IT professionals who have knowledge of fog computing and zero trust security believed that zero trust security and MFA in a fog computing environment (a) are easy to use, (b) promote their job efficiency, (c) are more secure than traditional security methods, and (d) they would be comfortable recommending implementation in their organization. Though there are security issues in fog computing technology as per the literature and still in the early implementation stages at the enterprise level, the population of this research study believes that robust security mechanisms such as zero trust security and MFA would be beneficial when implemented in the fog computing environment at the enterprise level. This research study could help organizations consider security mechanisms seriously and implement a fog computing environment in their network.

REFERENCES

[1] P. Kumar and R. Kumar, “Issues and Challenges of Load Balancing Techniques in Cloud Com-puting: A Survey,” ACM Comput. Surv, vol. 51, 2019, doi: 10.1145/3281010.

[2] S. Kunal, A. Saha, and R. Amin, “An overview of cloud‐ fog computing: Architectures, applications with security challenges,” Security and Privacy, vol. 2, no. 4, Jul. 2019, doi: 10.1002/spy2.72.

[3] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, “A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges,” IEEE Communications Surveys and Tutorials, vol. 20, no. 1. Institute of Electrical and Electronics Engineers Inc., pp. 416–464, Jan. 01, 2018,doi: 10.1109/COMST.2017.2771153.

[4] S. Khan, S. Parkinson, and Y. Qin, “Fog computing security: a review of current applications and security solutions,” Journal of Cloud Computing, vol. 6, no. 1. Springer Verlag, Dec. 01, 2017,doi: 10.1186/s13677-017-0090-3.

[5] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, and O. Rana, “Fog computing for the Internet of Things: A survey,” ACM Trans Internet Technol, vol. 19, no. 2, Apr. 2019, doi: 10.1145/3301443.

[6] Y. I. Alzoubi, V. H. Osmanaj, A. Jaradat, and A. Al‐ Ahmad, “Fog computing security and privacy for the Internet of Thing applications: State‐ of‐ the‐ art,” Security and Privacy, vol. 4, no. 2, Mar. 2021, doi: 10.1002/spy2.145.

[7] L. Chen, Z. Dai, M. Chen, and N. Li, “Research on the Security Protection Framework of Power Mobile Internet Services Based on Zero Trust,” in Proceedings - 2021 6th International Conference on Smart Grid and Electrical Automation, ICSGEA 2021, Institute of Electrical and Electronics Engineers Inc., May 2021, pp. 65–68,doi: 10.1109/ICSGEA53208.2021.00021.

[8] D. Tyler and T. Viana, “Trust no one? A framework for assisting healthcare organisations in transitioning to a zero-trust network architecture,” Applied Sciences (Switzerland), vol. 11, no. 16, Aug. 2021, doi: 10.3390/app11167499.

[9] Q. Yao, Q. Wang, X. Zhang, and J. Fei, “Dynamic Access Control and Authorization System based on Zero-trust architecture,” in PervasiveHealth: Pervasive Computing Technologies for Healthcare, ICST, Oct. 2020, pp. 123–127,doi: 10.1145/3437802.3437824.

[10] S. Ibrokhimov, K. L. Hui, A. A. Al-Absi, H. J. Lee, and M. Sain, “Multi-factor authentication in cyber physical system: A state of art survey,” IEEE, 2019, doi: 10.23919/ICACT.2019.8701960.

[11] J. Ren, D. Zhang, S. He, Y. Zhang, and T. Li, “A survey on end-edge-cloud orchestrated network computing paradigms: Transparent computing, mobile edge computing, fog computing, and cloudlet,” ACM Computing Surveys, vol. 52, no. 6. Association for Computing Machinery, Oct. 01, 2019,doi: 10.1145/3362031.

[12] M. Muhammad, T. Alyas, F. Ahmad, F. Butt, W. Qazi, and S. Saqib, “An analysis of security challenges and their perspective solutions for cloud computing and IoT,” ICST Transactions on Scalable Information Systems, p. 166718, Jul. 2020, doi: 10.4108/eai.23-10-2020.166718.

[13] M. Al-Khafajiy, T. Baker, H. Al-Libawy, Z. Maamar, M. Aloqaily, and Y. Jararweh, “Improving Fog Computing Performance via Fog-2-Fog Collaboration,”Future Generation Computer Systems, vol. 100, 2019,doi: 10.1016/j.future.2019.05.015

[14] K. Tange, M. de Donno, X. Fafoutis, and N. Dragoni, “A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities,” IEEE Communications Surveys and Tutorials, vol. 22, no. 4, pp. 2489–2520, Oct. 2020, doi: 10.1109/COMST.2020.3011208.

[15] C. M. Chen, Y. Huang, K. H. Wang, S. Kumari, and M. E. Wu, “A secure authenticated and key exchange scheme for fog computing,” Enterp Inf Syst, vol. 15, no. 9, pp. 1200–1215, 2021, doi: 10.1080/17517575.2020.1712746.

[16] J. Ni, K. Zhang, X. Lin, and X. S. Shen, “Securing Fog Computing for Internet of Things Applications: Challenges and Solutions,” IEEE Communications Surveys and Tutorials, vol. 20, no. 1, pp. 601–628, Jan. 2018, doi: 10.1109/COMST.2017.2762345.

[17] G. Javadzadeh and A. M. Rahmani, “Fog Computing Applications in Smart Cities: A Systematic Survey,” Wireless Networks, vol. 26, no. 2, pp. 1433–1457, Feb. 2020, doi: 10.1007/s11276-019-02208-y.

[18] M. Mukherjee et al., “Security and Privacy in Fog Computing: Challenges,” IEEE Access, vol. 5, pp. 19293–19304, Sep. 2017, doi: 10.1109/ACCESS.2017.2749422.

[19] E. Alemneh, S. M. Senouci, P. Brunet, and T. Tegegne, “A two-way trust management system for fog computing,” Future Generation Computer Systems, vol. 106, pp. 206–220, May 2020, doi: 10.1016/j.future.2019.12.045.

[20] J. Gabris and J. W. Chapman, “Zero Trust Security,” inApress, 2021,doi: 10.1007/978-1-4842-6702-8.

[21] M. Shore, S. Zeadally, and A. Keshariya, “Zero Trust: The What, How, Why, and When,” Computer (Long Beach Calif), vol. 54, no. 11, pp. 26–35, Nov. 2021, doi: 10.1109/MC.2021.3090018.

[22] S. Mehraj and M. T. Banday, “Establishing a Zero Trust Strategy in Cloud Computing Environment,” 2020 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-6, 2020, doi: 10.1109/ICCCI48352.2020.9104214.

[23] S. Teerakanok, T. Uehara, and A. Inomata, “Migrating to Zero Trust Architecture: Reviews and Challenges,” Security and Communication Networks, vol. 2021. Hindawi Limited, 2021,doi: 10.1155/2021/9947347.

[24] M. Sultana, A. Hossain, F. Laila, K. A. Taher, and M. N. Islam, “Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology,” BMC Medical Informatics and Decision Making, vol. 20, no. 1, Oct. 2020, doi: 10.1186/s12911-020-01275-y.

[25] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-factor authentication: A survey,” Cryptography, vol. 2, no. 1, pp. 1–31, Mar. 2018, doi: 10.3390/cryptography2010001.

[26] E. E. Nwabueze, I. Obioha, and O. Onuoha, “Enhancing Multi-Factor Authentication in Modern Computing,” Communications and Network, vol. 09, no. 03, pp. 172–178, 2017, doi: 10.4236/cn.2017.93012.

[27] C. Jacomme and S. Kremer, “An Extensive Formal Analysis of Multi-factor Authentication Protocols,” ACM Transactions on Privacy and Security, vol. 24, no. 2, Feb. 2021, doi: 10.1145/3440712.

[28] S. al Harbi, T. Halabi, and M. Bellaiche, “Fog Computing Security Assessment for Device Authentication in the Internet of Things,” in Proceedings - 2020 IEEE 22nd International Conference on High Performance Computing and Communications, IEEE 18th International Conference on Smart City and IEEE 6th International Conference on Data Science and Systems, HPCC-SmartCity-DSS 2020, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 1219–1224,doi: 10.1109/HPCC-SmartCity-DSS50907.2020.00202.

[29] J. Bavishi, M. S. Shaikh, and R. Patel, “Scalable and Efficient Mutual Authentication Strategy in Fog Computing,” in Proceedings - 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2020, Institute of Electrical and Electronics Engineers Inc., Aug. 2020, pp. 77–83,doi: 10.1109/MobileCloud48802.2020.00019.

[30] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, “Fog Computing for the Internet of Things: Security and Privacy Issues,” IEEE Internet Comput, vol. 21, no. 2, pp. 34–42, Mar. 2017, doi: 10.1109/MIC.2017.37.

[31] F. D. Davis, “Perceived usefulness, perceived ease of use, and user acceptance of information technology,” MIS Quarterly, vol. 13, no. 3, pp. 319-340, 1989, doi: 10.2307/249008.

[32] H. G. Dawson, “Clearing the Clouds: Factors of Technology Adoption and Their Relationship to Cloud Computing Adoption in Unites States Higher Education – An Extended TAM Study,” Ph.D. Dissertation, Capella University, Minneapolis, MN, USA, 2015.

[33] G. B. Newman, “Facters Affecting the Slow Adoption of Edge Computing in the United States: A Quantitative Study,” Ph.D. Dissertation, Capella University, Minneapolis, MN, USA, 2020.

[34] A. Field, “Discovering Statistics Using IBM SPSS Statistics 2,” in 5th ed., Sage Publications, 2018.

[35] W. P. Vogt, “Quantitative research methods for professionals,” in Pearson Education, 2007.

[36] D. George, and P. Mallery, “IBM SPSS statistics 26 step by step: A simple guide and reference,” in Routledge, 2019, doi: 10.4324/9780429056765.

[37] J. Cohen, “Statistical power analysis for the behavioral sciences,” in 2nd ed., Lawrence Erlbaum Associates, 1988, doi: 10.4324/9780203771587.

[38] R. Kelter, “Bayesian alternatives to null hypothesis significance testing in biomedical research: A non-technical introduction to Bayesian inference with JASP,” BMC Medical Research Methodology, vol. 20, pp. 1-12, 2020, doi: 10.1186/s12874-020-00980-6.

[39] M. E. J. Masson, “A tutorial on a practical bayesian alternative to null-hypothesis significance testing,” Behavior Research Methods, vol. 43, pp. 679–690, 2011,doi: 10.3758/s13428-010-0049-5.

[40] D. van den Bergh et al., “A tutorial on Bayesian multi-model linear regression with BAS and JASP,” Behavior Research Methods, vol. 53, no. 6, pp. 2351–2371, Dec. 2021, doi: 10.3758/s13428-021-01552-2.

[41] R. van de Schoot, and S. Depaoli, “Bayesian analyses: Where to start and what to report,” The European Health Psychologist, vol. 16, no. 2, pp. 75-84, 2014.

[42] M. Al-Khafajiyet al., “COMITMENT: A Fog Computing Trust Management Approach,” Journal of Parallel and Distributed Computing, p.137, 2020,doi: 10.1016/j.jpdc.2019.10.006