Secure Biometric-Based Authentication For Multi-Level Authentication Cloud Computing

Sudhakar Godi, Rajasekhara Rao
Department of CSE, College of Engineering, Acharya Nagarjuna University, Guntur. Kurra,
Department of CSE, Usha Rama College of Engineering and Technology, Telaprolu.

ABSTRACT:
In a wired network, security protocols such as encryption, authentication, and other methods are recognized as standards by the industry. Even so, there seems to be no data given mostly on financial impact of integrating such procedures in a wireless connection. Moreover, there is just no assessment of how effectively a wireless communication interacts along with conventional security mechanisms like firewalls, authentication, or encryption. Any protection policy's effectiveness is measured by whether or not it is actionable and with what price. Previous analysis has focused on network security enforcement methods, but the impact of protection "cost" on efficiency but administration is still hasn't been assessed. Objectives of the analysis are to recognize security and achievement problems in wireless devices, as well as flaws in IEEE 802.11 WLAN service. A test plan was set up to determine current security solutions including its impacts on network performance for measuring the influence of security on performance. The file transfer protocol along with the hypertext transfer protocol is the two widely used data transfer protocols that were tested in accordance with various security mechanisms. For the different implementation protocols, this study quantified critical output variables such as response time and throughput.

Article Received: 18 October 2020, Revised: 3 November 2020, Accepted: 24 December 2020

Introduction

The experiment put each model to the test at various levels of defense. This protection levels were gradually enforced. Authentication, permission, and encryption protocols are used in the security setups. The security thresholds were chosen in a systematic displaying the authentication methods present for each of the 802.11 and 802.1X specifications. This model would be addressed to here as 802.1X standard from now on. This model's nine security thresholds are as follows: 1st level The security configuration setup plans offered is "no security." With the activated form, no authentication feature is allowed [1]. Step 2 MAC address authorization: The level performs MAC address verification only at access point. Wired Equivalence Privacy (WEP) Level 3 Authorization: That would be the mutual secret authentication method that is defined in the IEEE 802.11 protocol. Level 4 WEP authorization for 40-bit WEP authentication ensures data protection by integrating the encryption algorithm. 128-bit WEP encryption with Level 5 WEP authentication: the 128-bit public key utilized here must be established. Level 6 EAP-MD5 encryption: It denotes a password/username authentication system that is part of the 802.1X protocol [2].

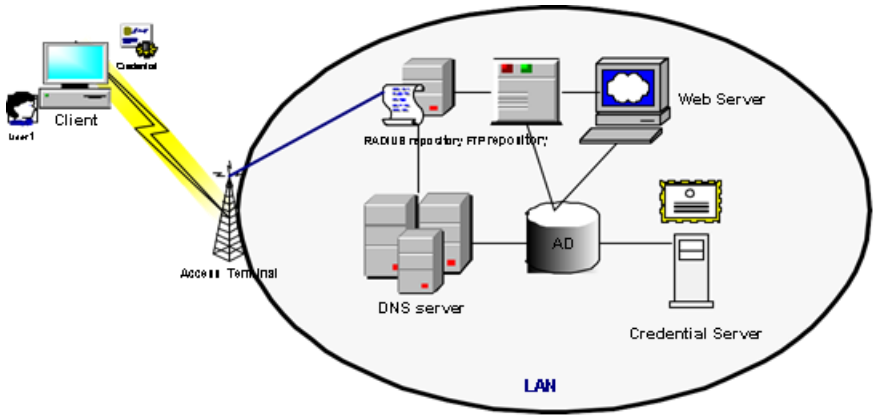

Fig 1 Framework Execution for 802.1X

802.1X supports Stage 7 Employee Assistance Program-Transport Layer Security (EAP-TLS) authorization, which is a PKI-dependent authorization tool. The cumulative impact of stage 8 EAP-MD5 along with 128-bit WEP authentication offers good data security[3]. The combination of stage 9 EAP-TLS including 128-bit WEP encoding provides a strong level in authentication and encryption utilizing each-session key. The 802.1X model's Security Levels 2 to 5 are compliant with the IEEE 802.11 specification. The 802.1X protocol has security levels 6 to 9.

Model of Virtual Private Network (VPN)

Based on the IPSec suite, we describe the VPN Model. Tunneling is accomplished using L2TP/IPSec (IPSec's transport mode option), that developers relate to only as IPSec tunneling innovation. Microsoft's terminal-to-terminal IPSec approach is available here. In our tests, we used two different forms of authentication methods: PKI with X.509 certificates is used for authentication scheme. Challenge Handshake Authentication Protocol (CHAP) along with EAP-TLS were chosen as consumer security protocols based on open-standards. The authentication mechanisms used in the 802.1X model can be directly compared with these two methods. PPTP was chosen as a reference to tunneling techniques in terms of efficiency [4][5]. In his study, discovered which L2TP/IPSec (Layer 2 Tunneling Protocol/Internet Protocol Security) routing had better output operating costs than PPTP (Point-to-Point-Tunneling-Protocol) . There are a decade degrees of security: 1st level, The default security setting is "no defense." This is something that the both 802.lX along with VPN versions see in general. Authorized tunnel provided utilizing PPTP tunneling along with CHAP encryption at stage 2 PPTP tunneling using CHAP. IPSec tunneling at level 3 and CHAP authentication: encrypted tunnel utilizing IPSec tunnel as well as CHAP encryption. Level 4 Firewall including PPTP along with CHAP: integrating firewall in funneling internet congestion into the architecture. Level 5 Firewall including IPSec along with CHAP: In an IPSec-based network, a firewall is mounted. Both protection levels after this one will be based on the IPSec architecture[6][7]. Stage 6 Using client PKI and node-dependent credential protection on a Level 6 Firewall for IPSec along with EAP-TLS. Stage 7 IPSec for CHAP along with DES: IPSec for CHAP user authentication uses DES encryption. Stage 8 DES encryption is used for

EAP-TLS authentication process in Level 8 IPSec for EAP-TLS and DES. Level 9 IPSec for CHAP along with 3DES: the best authentication (3DES) for CHAP is given. Tier 10 IPSec including EAP-TLS along with 3DES: uses the best security and device authentication mechanisms to encrypt data flow. Levels of security 2 to 4 encrypt data along with tunneling either using PPTP or L2TP or IPSec pre and post firewalls, and confidentiality mechanisms 2 to 4 include encryption along with tunneling either utilizing PPTP or L2TP or IPSec following the firewalls. For authentication and encryption at Levels of security from 5 to 10, an IPSec framework including firewalls is needed.

Implementation of the 802.1X Standard

The 802.11 entry protocol utilized shared key authorization, WEP encoding, including an 802.1X port-dependent encryption in the 802.1X prototype. The approach showed a managed wireless network featuring user identification, centrally controlled verification, including complex network distribution by incorporating 802.1X and 802.11 standards. Protection levels 2 to 5 were checked for the 802.11 entry protocol. The access point made static key control and simple network access easier[8][9][10]. The combination of 802.1X along with 802.11 supported cryptographic key management and integrated authorization through the Remote system for security levels 6 to 9. The EAP-MD5 including EAP-TLS ways of supporting were selected for the experiment; certain patented ways of supporting including EAP-TTLS also weren't included. Since WEP only guaranteed anonymity and secrecy on the wireless connection, but not on the wired equivalents, the whole paradigm didn't support terminal-to-terminal encryption. Wireless subscribers were handled as though they were members of a single intranet sub-network. The wireless customer, AP, and various server components were each given a unique IP address. To support 802.1X authentication, a RADIUS repository and credential administrators have been included in conceptual model. The assign responsibilities has been used to issue credentials to clients with EAP-TLS authorization, and the RADIUS repository enabled wireless user sign-on[11].

Implementation of the VPN Model

To support terminal-to-terminal encrypted connectivity through wireless to wired links, the VPN prototype utilized the IPSec method. IPSec and PPTP were used as tunneling protocols. The IPSec mechanism was used for the bulk of the research. We checked the results of utilizing PPTP tunneling towards IPSec in the initial phase since PPTP denotes to a common VPN tunneling option utilized by firms. To recognize a recipient, PKI was chosen over pre-shared keys, whereas X.509 credentials were utilized in dispensing and validating the key code. CHAP and EAP- TLS were chosen as user authentication options. CHAP authentication is the same as EAP-MD5 authentication. In protection levels 2 to 5, password protection including tunneling methods was evaluated pre and post firewall deployment. From then on, IPSec has been the only security protocol supported, along with a variety of client authorization options. Both user and system authentication is available at security levels 3 and 5 to 10. To guarantee terminal-to-terminal data protection, encryption methods such as DES and 3DES were used. The infrastructure was split in sub-networks, with the cellular sub-network often treated as an extranet[12].

Additional Ingredients

New functionalities were connected to the network in the VPN model, including a RADIUS registry, VPN repository, credential management, including firewall. During the 802.1X model test, the RADIUS database and certification authorities have been installed; thus, just a VPN repository and a firewall became installed for the first time. We set up a software firewall between both the access points along with the VPN database and configured the VPN server to become the RADIUS (Remote Authentication Dial-In User Service) operator. Our first option had been a hardware firewall; however, vendor product interoperability problems arose. As a result, a software firewall was installed[13].

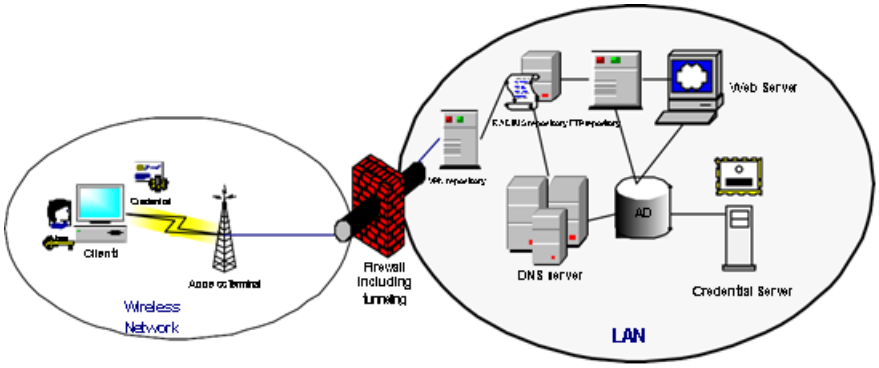

Fig 2 Framework implementation for VPN framework

Methodology

The process and atmosphere used to perform the experiments for this study are mentioned. The experiments' goal is to measure the effect of protection on 802.11b WLAN outcomes. The 2 AAA (Authentication, Authorization and Accounting) WLAN frameworks viz. the 802.1X along with the VPN were chosen as the two protection methodologies to determine the extent of service interruption. The 802.1X framework combines the fundamental security of the 802.11 standard with the WEP protocol, as well as the improved security of the 802.1X standard with the EAP protocol. For end-to-end encryption, the VPN model provides the IPSec protocol set. To conduct the experiment, each security model was designed with a series of security layers. There are significant variations here between the two approaches: the VPN framework enables end devices to enforce the authentication system, while the 802.1X methods depend in accordance with the terminal point (in the form of authentication system) to provide assistance[14][15.

Evaluation and Analysis of Experiments

We calculate the amount of performance overhead experienced when applying the various protection measures mentioned in Chapter 5 in this chapter. We aim to discuss the impact of protection levels, templates, and traffic forms on efficiency in particular. Experimenting with different protection protocol deployments, as well as varying variations of these mechanisms, was used to conduct data analysis. The data obtained from the experiment was analyzed using statistical methods such as analysis of variance (ANOVA) and t-tests for analysis instruments). In order to develop wireless security solutions, the analyzed findings would be paired only with information security and other efficiency criteria[16].

Overview of the Experiment

The tests were conducted using the 802.1X and VPN versions. For a single customer, an application model of service as well as a unit cell has been used. For each standard, performance data was gathered by repeating ten experiments with various security configurations. The Ethereal tracking tool collected FTP and HTTP traffic. The 95 percent confidence interval was used to analyze the data. The following null and alternate hypotheses were formed to address our study questions: There are no differences between both the designs utilized in securing WLAN communication. The other postulation would require the VPN interface degrading efficiently rather than the 802.1X model. The t-test was used to run statistical analyses. There is no distinction between different modes of traffic, although the alternate explanation suggests that there is. The t-test was used to run statistical analysis. The alternate hypothesis suggests that there is a distinction between the protections measures used for each prototype, whereas the initial hypothesis suggests that there is ANOVA that was used to conduct statistical analyses, which were supplemented by different t-tests.

Re-examination

The information from either the VPN experiments performed yielded unpredictable findings. The findings of levels of security from 4 to 5, along with 7 to 10 didn't endorse the hypothesis which enhanced that the confidential approaches had a stronger impact on getting the outputs. We discovered that:

i) The use of a firewall increased the performance of the network.

ii) User authentication for CHAP took longer than EAP-TLS authentications.

iii) When opposed to DES encryption, 3DES encryption boosted HTTP throughput.

To find out what was causing these protection thresholds to malfunction, retesting was done. We chose to restart the devices any moment an IPSec protocol is modified, preventing the existence of previous IPSec policies. Just the firewall security standards produced roughly the same findings pre and post retesting, according to a comparison of the data obtained before and after retesting; the other security levels followed our assumptions. As a result, we came to the conclusion that when changing IPSec policies/filters, such as switching via DES to 3DES, software system must be rebooted to avoid side affects with prior policy development.

The Effect of Model Selection

The experiment's observations contradicted the null hypothesis, suggesting that the VPN paradigm resulted in better output fixed costs. Figures 3 and 4 shows that with the FTP and HTTP traffic, the VPN model has longer reaction times and lower throughputs on an average.

Table 1 Mean Reaction Time and Throughput for the Two Approaches

Approach	**802.1X framework**		**VPN framework**	
(Mean)	Reaction Time	Throughput	Reaction Time	Throughput
File Transfer Protocol	20.016	977821651	42.586	38554.333
	26.834	20641.365	49.852	13561.028

Hyper Text Transfer Protocol				

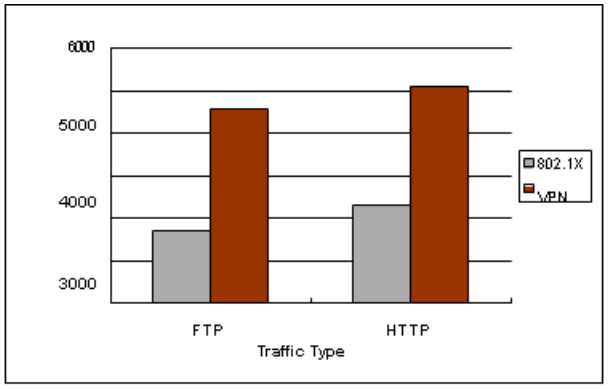

Fig 3 Mean reaction time for the two methodologies

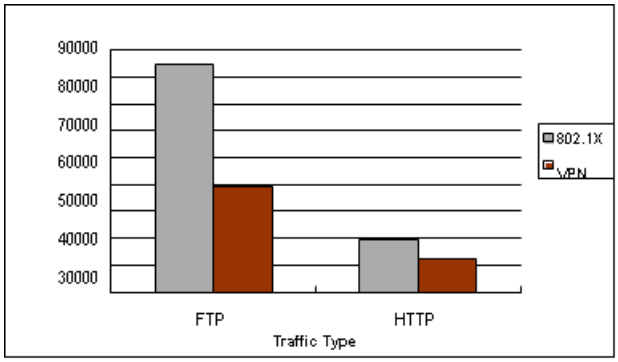

Fig 4 Mean throughput for the two methodologies

Table 2 shows that using new approaches to protect wireless transmission had a major impact on efficiency, with a p value of 0.0001, irrespective on what activity systems would be used. For both FTP and HTTP traffic, the VPN template had about double the connection speed. For FTP communications, the 802.1X framework supported considerably higher throughput. Tunneling, intrusion detection, sensor credential verification, advanced key sharing, and data encryption were all used to help mitigate the performance degradations.

Impact of Traffic Type on Performance

FTP and HTTP were the two main categories of program standards used to transmit files in each model. FTP is often used to transmit big files, while HTTP sends and receives a sequence of request-response messages during the transmission process. FTP reaction time and performance were comparable to HTTP for each design. Table 3 demonstrates the influence of multiple traffic models on efficiency by each method; the p-ratings were lower when compared with the alpha rating of 0.04, indicating that the kind of congestion utilized had a major impact on overall network performance.

Model	FTP		HTTP	
t -statistics p -value	ReactionTime Throughput		ReactionTime Throughput	
	-9.1813	8.6089	-9.1132	8.4091
	0.0000	0.0000	0.0000	0.0000

Table 2 Comparison of framework 801.1X and VPN for HTTP and FTP

As seen in Table 7-1, FTP outperformed HTTP, with a quicker response time and higher throughput. The table also demonstrated that the 802.1X framework outperformed the VPN framework. This table only gives a small perspective due to the complexities of these transmitting methods and the various file sizes used. Impact of Security Levels contains more detailed analyses of traffic type impacts.

Congestion	802.1X Framework		VPN Framework	
t-statistics p-value	Reaction Time Throughput		Reaction Time Throughput	
	-28.0239	17.4831	-9.7957	11.5024
	0.0000	*0.0000*	*0.0000*	*0.0000*

Table 3 FTP and. HTTP Results for the 2 Models

ANOVA was used to analyze the data obtained from the trials, evaluating the overall effect of the different parameters (safety measures in relation to network traffic) on results in the two models. ANOVA, on the other hand, does not offer reasons for inconsistencies or a thorough understanding of experiences. Using paired t-tests allows for a more thorough study of the effect of various protection levels on results.

Differences in Defense Standards in General

To assess the overall protection standards and traffic type effect within each model, four two-way ANOVA tests were performed. The ANOVA looked at the results of two components: protection standards (across each method) and activity sort, and saw how there was an association effect between them. Table 7-4 indicates that important association effects between these two variables were observed at the 0.05 stage for each model. As a result, network efficiency is influenced by both security levels and traffic types (response times and throughputs). As a result, the actual key effects on output (in each attribute) just cannot be viewed differently. In most cases, while evaluating the effect on efficiency, both the protection level and the forms of traffic must be weighed. The findings of the ANOVA provide ample objective proof that the protection thresholds used on this role assigned differently. The waiting times including bandwidths related to different congestion categories (HTTP along with FTP) revealed how protection standards have a large influence on efficiency (p-value of 0.0000); see Table 4 for more information.

ANOVA	802.1X Model				
		Reaction Time		Throughput	
	df	F-ratio	p value	F-ratio	p value
Security Levels (x)	8	2737.25	0.0000	692.14	0.0000
Traffic Types (y)	1	1542.53	0.0000	14662.81	0.0000
Interaction (x*y)	8	12.91	0.0000	451.67	0.0000
	VPN Model				
		Reaction Time		Throughput	
	df	F ratio	p-value	F ratio	p-value
Security Levels (x)	9	1600.16	0.0000	997.31	0.0000
Traffic Types (y)	1	164.80	0.0000	5647.17	0.0000
Interaction (x*y)	9	10.31	0.0000	458.92	0.0000

Table 4 ANOVA Analysis for entire Security Levels

Conclusion

Performance expenses for different security protocols were explored in our experimental study, and we discovered the more secure an infrastructure is, the more efficiency was affected. As predicted, the VPN model degraded efficiency more than just the 802.1X framework; the VPN framework supported device-to-device protection by using dual security (gadget and client), an advanced encryption mechanism, improved key storage, and tunneling technologies.

Authorization (HTTP) frameworks generated additional accomplishment overheads versus FTP, as the link between the two nodes improved based on security agreement and administration. Apart from the situation of MAC address authorization, WEP user authentication, a firewall, including 3DES cryptography in the VPN framework, our assessment of different protection levels revealed that now the stronger the protection standard (because as system have become more stable), the greater the efficiency price generated.

More study is needed to look at the impact of a hardware or software gateway on the infrastructure, and also various traffic patterns in different cryptography techniques.

References

1. Alezabi, K.A., Hashim, F., Hashim, S.J. *et al. 2020.* Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks. *J Wireless Com Network,* 105. https://doi.org/10.1186/s13638-020-01702-8
2. Easttom W. 2021. Virtual Private Networks, Authentication, and Wireless

Security. In: Modern Cryptography. Springer, Cham. https://doi.org/10.1007/978-3-030-63115-4_14

3. Khedr, W.I., Hosny, K.M., Khashaba, M.M. *et al. 2020.* Prediction-based secured handover authentication for mobile cloud computing. *Wireless Netw* **26,** 4657–4675. https://doi.org/10.1007/s11276-020-02368-2
4. Lee, D.H., Kim, J.G. 2014 IKEv2 authentication exchange model and performance analysis in mobile IPv6 networks. *Pers Ubiquit Comput* **18,** 493–501 (2014). https://doi.org/10.1007/s00779-013-0669-8
5. Pahlavan, K., Krishnamurthy, P. 2021. Evolution and Impact of Wi-Fi Technology and Applications: A Historical Perspective. *Int J Wireless Inf Networks* **28,** 3–19. https://doi.org/10.1007/s10776-020-00501-8
6. Ribeiro, M., Nunes, N., Nisi, V. *et al. 2020.* Passive Wi-Fi monitoring in the wild: a long-term study across multiple location typologies. *Pers Ubiquit Comput*. https://doi.org/10.1007/s00779-020-01441-z
7. Anil Kumar Biswal, Debabrata Singh, Binod Kumar Pattanayak, Debabrata Samanta, Ming-Hour Yang, "IoT-Based Smart Alert System for Drowsy Driver Detection", Wireless Communications and Mobile Computing, vol. 2021, Article ID 6627217, 13 pages, 2021. https://doi.org/10.1155/2021/6627217.
8. M. Maheswari, S. Geetha, S. Selva kumar, M. Karuppiah, D. Samanta and Y. Park, "PEVRM: Probabilistic Evolution based Version Recommendation Model for Mobile Applications," in IEEE Access, doi: 10.1109/ACCESS.2021.3053583 .
9. Gomathy, V., Padhy, N., Samanta, D. et al. Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks. J Ambient Intell Human Comput 11, 4995–5001 (2020). https://doi.org/10.1007/s12652-020-01797-3.
10. Sivakumar, P., Nagaraju, R., Samanta, D. et al. A novel free space communication system using nonlinear InGaAsP microsystem resonators for enabling power-control toward smart cities. Wireless Netw 26, 2317–2328 (2020). https://doi.org/10.1007/s11276-019-02075-7.
11. Khamparia, A, Singh, PK, Rani, P, Samanta, D, Khanna, A, Bhushan, B. An internet of health things-driven deep learning framework for detection and classification of skin cancer using transfer learning. Trans Emerging Tel Tech. 2020;e3963. https://doi.org/10.1002/ett.3963 .
12. Althar, R.R., Samanta, D. The realist approach for evaluation of computational intelligence in software engineering. Innovations Syst Softw Eng (2021). https://doi.org/10.1007/s11334-020-00383-2
13. Guha, A., Samanta, D. Hybrid Approach to Document Anomaly Detection: An Application to Facilitate RPA in Title

Insurance. Int. J. Autom. Comput. 18, 55–72 (2021). https://doi.org/10.1007/s11633-020-1247-y .

14. You, X., Wang, CX., Huang, J. *et al.* 2021. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. *Sci. China Inf. Sci.* **64,** 110301. https://doi.org/10.1007/s11432-020-2955-6
15. Zeleke, B.M., Brzozek, C., Bhatt, C.R. *et al.* 2021. Wi-fi related radiofrequency electromagnetic fields (RF-EMF): a pilot experimental study of personal exposure and risk perception. *J Environ Health Sci Engineer*. https://doi.org/10.1007/s40201-021-00636-7.
16. V. Dhanush, A. R. Mahendra, M. V. Kumudavalli and D. Samanta, "Application of deep learning technique for automatic data exchange with air-gapped systems and its security concerns," 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2017, pp. 324-328, doi: 10.1109/ICCMC.2017.8282701.