PERAN MEDIA PENYIARAN KOMUNIKASI ISLAM DALAM MEMBANGUN KESADARAN PUBLIK DI ERA DIGITAL

The Role of Islamic Communication Broadcasting Media in Building Public Awareness in the Digital Era

Muhammad Saleh[1] , Irda Maulida[2] , Oknita[3] ,Yuliana Restiviani[4] T. Faizin[5] , Kamaruzzaman[6]

Komunikasi dan Penyiaran Islam, Fakultas Dakwah
Institut Agama Islam Negeri Lhokseumawe
alamat institusi lengkap
*Email: [1]muhammadsaleh@iainlhokseumawe.ac.id
[2] syahiraokha@yahoo.co.id

ABSTRAK

Keamanan dalam komunikasi publik adalah aspek krusial yang memerlukan perhatian serius di era digital. Penelitian ini mengeksplorasi dan mengevaluasi protokoler keamanan yang ada dalam literatur terkini. Melalui studi pustaka, ditemukan tema-tema utama seperti metode keamanan, efektivitas protokol, serta tantangan dalam penerapannya. Selain itu, penelitian ini juga mengkaji peran media penyiaran komunikasi Islam dalam membangun kesadaran publik. Hasilnya menunjukkan bahwa meskipun ada protokol standar, masih terdapat inkonsistensi dan kesenjangan dalam penerapannya. Media penyiaran komunikasi Islam berperan penting dalam menyebarkan informasi yang relevan dan membangun kesadaran di kalangan masyarakat. Penelitian ini berkontribusi dalam mengidentifikasi area yang memerlukan penelitian lanjutan dan menawarkan rekomendasi untuk meningkatkan praktik keamanan komunikasi publi

***Kata Kunci**: Peran Media, Komunikasi Islam, Digital*

A. PENDAHULUAN

Keamanan dalam komunikasi publik menjadi sangat penting di era digital ini, di mana informasi tersebar dengan cepat dan mudah. Komunikasi publik sering kali mengandung informasi sensitif, seperti data pribadi, rahasia negara, atau informasi keuangan. Kebocoran informasi ini dapat berakibat fatal, seperti pencurian identitas, spionase, atau kerugian finansial. Kehilangan kepercayaan publik terhadap pemerintah atau organisasi dapat berakibat serius. Pelanggaran keamanan dapat merusak reputasi dan menghambat kelancaran operasi. Di Indonesia Pada tahun 2021, data pribadi 10 juta pengguna BPJS Kesehatan bocor. Hal ini menimbulkan kekhawatiran besar dan memicu tuntutan reformasi keamanan data. Kejadian serupa terjadi di Amerika Serikat, dimana pada tahun 2016, peretas Rusia diduga membobol server email Komite Nasional Demokrat (DNC) dan membocorkan email internal yang digunakan untuk mendiskreditkan kandidat presiden Hillary Clinton. dan pada tahun 2017, serangan ransomware WannaCry melumpuhkan sistem komputer di berbagai negara, termasuk Inggris, menyebabkan kerugian miliaran dolar.

Kerugian global akibat cybercrime mencapai USD 6 triliun pada tahun 2021 dan diprediksikan akan mencapai USD 10 triliun pada tahun 2025. Di Indonesia, berdasarkan

data Badan Siber dan Sandi Negara (BSSN), terdapat 23.028 kasus serangan siber di tahun 2022, meningkat 11,5% dibandingkan tahun 2021. Kasus-kasus dan data di atas menunjukkan bahwa keamanan dalam komunikasi publik bukan hanya isu sepele, tetapi memiliki dampak yang signifikan. Oleh karena itu, penting bagi pemerintah, organisasi, dan individu untuk mengambil langkah-langkah yang tepat untuk meningkatkan keamanan komunikasi publik.

B. LANDASAN TEORI

1. Definisi dan Konsep Keamanan dalam Komunikasi

Komunikasi adalah proses pertukaran informasi dan makna antara dua atau lebih pihak. Dalam proses ini, informasi dapat berupa ide, perasaan, atau pengalaman yang disampaikan melalui berbagai media, seperti bahasa verbal, nonverbal, atau media elektronik. Menurut Wilbur Schramm, Komunikasi adalah proses mentransfer makna dari pengirim ke penerima. Sedangkan Menurut Carl Hovland, Komunikasi adalah proses di mana seseorang (komunikator) menyampaikan pesan kepada orang lain (penerima) melalui media tertentu, baik lisan, tulisan, maupun visual, sehingga pesan tersebut dipahami oleh penerima. Hal ininjuga senada dengan pendapat Harold D. Lasswell yang menyebutkan bahwa komunikasi adalah proses di mana seseorang (komunikator) menyampaikan pesan kepada orang lain (penerima) melalui media tertentu (media) untuk mencapai efek tertentu (efek).

Keamanan dalam komunikasi adalah suatu keadaan di mana informasi yang dipertukarkan terjamin kerahasiaannya, integritasnya, dan ketersediaannya dari pihak-pihak yang tidak berwenang. Keamanan komunikasi sangat penting untuk melindungi informasi sensitif, mencegah pencurian data, dan menjaga privasi individu dan organisasi.(Ramadani, 2019)

Aspek-aspek Penting dalam Keamanan Komunikasi merupakan hal yang tidak bisa dianggap sepela, karena dapat mempengaruhi suatu informasi,

a. Kerahasiaan (Confidentiality)

Informasi hanya boleh diakses oleh pihak-pihak yang berwenang. Hal ini dapat dicapai dengan menggunakan metode enkripsi untuk melindungi data saat transit dan saat disimpan.

b. Integritas (Integrity)

Informasi harus terjamin keaslian dan keakuratannya. Hal ini dapat dicapai dengan menggunakan metode otentikasi dan verifikasi data.

c. Non-repudiation

Pengirim dan penerima informasi harus dapat membuktikan bahwa mereka telah terlibat dalam proses komunikasi. Hal ini dapat dicapai dengan menggunakan tanda tangan digital dan protokol logging.

d. Otorisasi (Authority)

Hanya pihak-pihak yang berwenang yang boleh mengakses dan memodifikasi informasi. Hal ini dapat dicapai dengan menggunakan kontrol akses dan manajemen identitas.

e. Ketersediaan (Availability)

Informasi harus tersedia bagi pihak-pihak yang berwenang saat dibutuhkan. Hal ini dapat dicapai dengan menggunakan infrastruktur IT yang handal dan menerapkan strategi redundansi data.

f. Privasi

Privasi individu dan organisasi harus dilindungi dari pengumpulan dan penggunaan data yang tidak sah. Hal ini dapat dicapai dengan menerapkan kebijakan privasi data yang kuat dan mematuhi peraturan perundang-undangan yang berlaku.

2. Protokoler Keamanan dalam Komunikasi Publik

Keamanan komunikasi publik menjadi semakin penting di era digital ini, di mana informasi sensitif dapat dengan mudah diretas dan disalahgunakan. Berbagai protokol keamanan telah dikembangkan untuk melindungi komunikasi publik, mulai dari protokol standar yang digunakan secara luas hingga solusi yang lebih canggih untuk kebutuhan khusus.(S. A. E. Dewi, 2021)

Para ahli keamanan informasi menekankan pentingnya menggunakan protokol keamanan yang kuat dalam komunikasi publik. Bruce Schneier, seorang pakar kriptografi terkemuka, menyatakan bahwa "keamanan bukanlah produk, melainkan sebuah proses." Dia menekankan pentingnya pembaruan perangkat lunak dan protokol keamanan secara berkala untuk mengikuti ancaman yang berkembang. Menurut Verizon Data Breach Investigations Report 2023, 83% pelanggaran data melibatkan faktor manusia, seperti phishing, rekayasa sosial, dan kesalahan manusia.(Saleh et al., 2021) Hal ini menunjukkan pentingnya edukasi dan pelatihan pengguna tentang praktik keamanan yang baik.(Priyatna et al., 2020)

Beberapa Protokol standar yang digunakan dalam komunikasi publik adalah;

a. Transport Layer Security (TLS) dan Secure Sockets Layer (SSL). TLS dan SSL adalah protokol keamanan yang digunakan untuk memastikan keamanan komunikasi antara klien dan server. TLS dan SSL menggunakan enkripsi dan autentikasi untuk mencegah akses tidak sah dan menghentikan serangan siber. TLS dan SSL juga menggunakan sertifikat digital untuk memverifikasi identitas server dan klien.

b. (HTTPS) Hypertext Transfer Protocol Secure adalah protokol dasar untuk komunikasi web yang aman. HTTPS menggunakan enkripsi Transport Layer Security (TLS) untuk melindungi data yang dikirim antara browser dan server web. TLS memastikan kerahasiaan, integritas, dan otentikasi data.(Prayama & Yolanda, 2021)

c. IPsec: Internet Protocol Security adalah suite protokol yang digunakan untuk mengamankan komunikasi jaringan IP. IPsec menyediakan enkripsi, otentikasi, dan kontrol akses untuk komunikasi antara perangkat di jaringan.(Andy & Rahardjo, 2018)

d. SMTPS: Simple Mail Transfer Protocol Secure adalah protokol email yang aman yang menggunakan TLS untuk melindungi data email saat transit. SMTPs membantu mencegah penyadapan email dan pemalsuan identitas pengirim.

e. SRTP: Secure Real-time Transport Protocol adalah protokol yang digunakan untuk mengamankan komunikasi multimedia, seperti panggilan suara dan video. SRTP menyediakan enkripsi, otentikasi, dan kontrol akses untuk komunikasi multimedia.(S. Dewi, 2020)

Banyak penelitian telah dilakukan untuk meningkatkan keamanan komunikasi publik *A Survey of Secure Multiparty Computation Protocols* oleh Dugan (2020) menyurvei berbagai protokol komputasi multipihak yang aman dan membahas aplikasi mereka dalam komunikasi publik.(Dugan & Zou, 2020) *Privacy-Preserving Machine Learning for Public Health Surveillance* oleh Fadila Zerka (2022) mengeksplorasi bagaimana pembelajaran mesin yang menjaga privasi dapat digunakan untuk memantau kesehatan masyarakat sambil melindungi privasi individu.(Zerka et al., 2020)

3. Risiko dan Ancaman dalam Komunikasi Publik

Komunikasi publik, sebagai proses penyampaian informasi kepada masyarakat luas, tak luput dari berbagai risiko dan ancaman. Ancaman ini dapat datang dari berbagai pihak dan dalam berbagai bentuk, baik online maupun offline.Risiko dan ancaman dalam komunikasi publik dapat berupa ancaman fisik, cyber, dan lain-lain.(Nguyen et al., 2015)

a) Ancaman cyber dapat berupa serangan siber yang dilakukan dengan cara mengenkripsi file, membuatnya tidak dapat diakses tanpa kunci dekripsi, atau dengan cara menyusup ke dalam komunikasi antara dua pihak. Ancaman cyber dapat merugikan secara finansial dan dapat menyebabkan kerugian data bagi bisnis dan sifatnya tidak tergantikan. Jenis ancaman cyber diantaranya;

   a. Peretasan. Upaya tidak sah untuk mengakses, mengubah, atau mencuri informasi sensitif.

   b. Penipuan Daring. Penipuan yang dilakukan melalui platform online untuk menipu korban agar menyerahkan informasi pribadi atau uang.

   c. Penyebaran Informasi Salah (Misinformasi dan Disinformasi). Penyebaran informasi yang keliru atau menyesatkan untuk memanipulasi opini publik.(Susanto & Handayani, 2008)

   d. Serangan Siber. Upaya untuk mengganggu, menonaktifkan, atau merusak sistem komunikasi publik.

b) Ancaman fisik dapat berupa serangan terhadap individu atau organisasi, seperti kekerasan, pencurian, atau penghancuran properti. Contoh ancaman fisik dapat berupa ; (1) Kekerasan, yaitu tindakan agresif yang bertujuan untuk melukai atau mencederai orang lain. (2) Vandalisme. Perusakan properti atau infrastruktur publik. (3) Gangguan: Upaya untuk mengganggu jalannya komunikasi publik, seperti demonstrasi anarkis.

c) Ancaman lain dapat berupa (1) ancaman social engineering, yang menggunakan manipulasi psikologis untuk memanipulasi individu agar mengungkapkan informasi rahasia atau melakukan tindakan tertentu. (2) Ancaman lain juga dapat berupa kejahatan siber yang melibatkan akses ilegal dan pengambilan data pribadi atau korporat, seperti pencurian data. (3)Ketidakpercayaan Publik. Dimana Kehilangan kepercayaan masyarakat terhadap informasi yang disampaikan oleh pemerintah atau lembaga publik. (4) Polarisasi Politik yang dapat memperparah perpecahan politik dan mempersempit ruang dialog konstruktif. (5)

Ketidakstabilan Sosial, sehingga dapat menimbulkan keresahan dan kekacauan dalam masyarakat.

Dampak dari ancaman-ancaman tersebut dapat sangat merugikan dan berdampak fatal, seperti (1) Kerugian Finansial. Kebocoran data sensitif dapat menyebabkan kerugian finansial bagi individu dan lembaga. (2) Kerusakan Reputasi. Penyebaran informasi salah dan serangan siber dapat merusak reputasi pemerintah dan lembaga publik. (3) Kerusuhan Sosial. Gangguan dan kekerasan dapat memicu kerusuhan sosial dan mengancam stabilitas keamanan. (4) Terhambatnya Komunikasi Publik. Ancaman-ancaman ini dapat menghambat upaya pemerintah dan lembaga publik untuk menyampaikan informasi penting kepada masyarakat.

Strategi pencegahan ancaman-ancaman tersebut dapat dilakukan dengan memahami berbagai jenis ancaman dan mengambil tindakan preventif. Contohnya, memahami berbagai jenis ancaman cybersecurity dan mengambil tindakan preventif seperti menimba ilmu pendidikan dan kesadaran mengenai ancaman cybersecurity, pembaruan dan patching sistem secara berkala, penggunaan antivirus dan anti-malware, pengaktifan otentikasi dua faktor, penggunaan VPN, dan rutin melakukan backup data.(Mujiastuti & Prasetyo, 2021) Dalam komunikasi risiko, strategi pencegahan juga dapat dilakukan dengan membangun kesadaran publik akan adanya bahaya (risiko) dan melakukan persuasi kepada publik agar melakukan tindakan untuk mencegah terjadinya risiko/bahaya.

4. Evaluasi Keamanan

Evaluasi keamanan dalam komunikasi publik merupakan proses yang berkelanjutan untuk mengidentifikasi, menganalisis, dan menilai risiko keamanan yang terkait dengan aktivitas komunikasi publik. Prosedurnya umumnya meliputi beberapa langkah berikut;

a) Penentuan Ruang Lingkup: Menetapkan batasan dan fokus evaluasi, termasuk jenis komunikasi publik, platform yang digunakan, dan audiens yang ditargetkan.

b) Identifikasi Ancaman: Menentukan potensi ancaman keamanan yang dapat membahayakan komunikasi publik, seperti peretasan, penyalahgunaan data, penyebaran informasi keliru, dan gangguan.

c) Analisis Kerentanan: Menilai kerentanan sistem dan proses yang digunakan dalam komunikasi publik yang dapat dieksploitasi oleh ancaman yang diidentifikasi.

d) Penilaian Risiko: Menentukan tingkat risiko yang terkait dengan setiap ancaman dan kerentanan, dengan mempertimbangkan kemungkinan dan dampak potensial.

e) Penetapan Pengendalian: Mengembangkan dan menerapkan langkah-langkah pengamanan untuk mengurangi risiko yang diidentifikasi, seperti enkripsi data, kontrol akses, dan edukasi pengguna.

f) Monitoring dan Evaluasi: Melakukan pemantauan berkelanjutan terhadap efektivitas langkah-langkah pengamanan dan melakukan evaluasi berkala untuk memastikan keamanan komunikasi publik tetap terjaga.

Berbagai metode dan alat dapat digunakan untuk mengevaluasi keamanan dalam komunikasi publik, di antaranya:

a) Penilaian Risiko: Metode formal untuk mengidentifikasi, menganalisis, dan menilai risiko keamanan.

b) Pengujian Penetrasi: Simulasi serangan siber untuk menguji kerentanan sistem dan proses.

c) Pemindaian Kerentanan: Pemeriksaan otomatis untuk menemukan kerentanan dalam sistem dan perangkat lunak.

d) Analisis Keamanan Kode: Peninjauan kode sumber untuk mengidentifikasi potensi kelemahan dan kerentanan.

e) Pemantauan Keamanan: Pelacakan aktivitas dan peristiwa keamanan untuk mendeteksi ancaman dan insiden.

Beberapa indikator kinerja keamanan yang dapat digunakan untuk mengukur efektivitas evaluasi dan langkah-langkah pengamanan dalam komunikasi publik, di antaranya:

a) Jumlah pelanggaran keamanan: Jumlah insiden keamanan yang terjadi, seperti peretasan, pencurian data, dan penyebaran informasi keliru.

b) Waktu pemulihan: Lama waktu yang dibutuhkan untuk memulihkan sistem dan layanan setelah insiden keamanan.

c) Kepuasan pengguna: Tingkat kepuasan pengguna terhadap keamanan komunikasi publik.

Kepatuhan terhadap peraturan: Tingkat kepatuhan terhadap peraturan dan standar keamanan yang terkait dengan komunikasi publik

C. METODE

Jenis penelitian yang digunakan penulis dalam penelitian ini adalah studi kepustakaan. Studi kepustakaan, menurut Syaibani (2012), adalah upaya peneliti untuk menghimpun informasi yang relevan dengan topik atau masalah yang sedang diteliti. Informasi ini tersedia dari berbagai sumber literatur akademik, laporan penelitian, karya ilmiah, disertasi, aturan-aturan, dan buku ilmiah. Sumber data dalam penelitian ini diperoleh dari literatur-literatur yang relevan dengan topik penelitian. Istilah data pustakaan tidak dibatasi oleh ruang dan waktu, memungkinkan penulis untuk mengakses berbagai sumber informasi dari masa lalu hingga masa kini yang berkaitan dengan Protokoler Keamanan, Komunikasi Publik, Evaluasi Keamanan, Eksplorasi Keamanan..

D. HASIL DAN PEMBAHASAN

Tingkat kepatuhan terhadap protokol keamanan dalam komunikasi publik bervariasi tergantung pada konteks dan faktor yang mempengaruhinya. Studi di Indonesia menunjukkan kepatuhan terhadap protokol keamanan siber dalam komunikasi publik masih rendah, dengan hanya 37,5% responden yang selalu mengikuti protokol. Studi di Indonesia mengenai kepatuhan terhadap protokol keamanan siber dalam komunikasi publik menunjukkan hasil yang rendah. Dalam survei yang dilakukan, hanya 37,5% responden yang selalu mengikuti protokol keamanan siber dalam komunikasi publik. Hal ini menunjukkan bahwa masih banyak orang yang tidak memperhatikan keamanan siber dalam berkomunikasi secara online, sehingga meningkatkan risiko serangan siber dan kerugian data. Dalam konteks manajemen komunikasi, keamanan siber menjadi sangat penting untuk memastikan komunikasi yang efektif dan aman. Manajer komunikasi harus

berinisiatif untuk mengatur dan mengatur rapat koordinasi secara berkala serta berkolaborasi dengan cepat untuk mengatasi masalah yang timbul dalam komunikasi.
Laporan "Public Communication Security Breaches: A Global Analysis": Laporan ini mencatat peningkatan insiden keamanan dalam komunikasi publik, seperti peretasan akun media sosial dan penyebaran informasi yang salah.

Kepatuhan individu terhadap protokol keamanan dipengaruhi oleh berbagai faktor. Artikel "The Role of Security Protocols in Public Communication": Penelitian di Amerika Serikat menemukan bahwa kepatuhan terhadap protokol keamanan komunikasi publik dipengaruhi oleh beberapa faktor, seperti tingkat keparahan ancaman, pemahaman individu tentang protokol, dan kepercayaan terhadap otoritas yang menetapkan protokol. Salah satu faktor utama adalah tingkat keparahan ancaman yang dirasakan. Ketika individu memahami bahaya yang ditimbulkan oleh pelanggaran keamanan, mereka cenderung lebih patuh terhadap protokol yang ada. Pemahaman yang jelas tentang protokol juga memainkan peran penting; individu yang mengerti apa yang harus dilakukan dan mengapa hal itu penting lebih mungkin untuk mengikuti aturan yang ditetapkan. Selain itu, kepercayaan terhadap otoritas yang menetapkan protokol merupakan faktor krusial. Jika individu percaya bahwa otoritas tersebut kompeten dan memiliki niat baik, mereka akan lebih cenderung mematuhi instruksi yang diberikan. Budaya organisasi juga memiliki dampak signifikan; organisasi yang menekankan pentingnya keamanan dan membangun lingkungan kerja yang mendukung kepatuhan akan mendorong individu untuk mengikuti protokol. Terakhir, teknologi yang mudah digunakan dan aman dapat meningkatkan kepatuhan. Ketika individu memiliki akses ke alat dan sistem yang membantu mereka mengikuti protokol dengan lebih mudah, mereka akan lebih cenderung mematuhi aturan yang ada.

Kejadian dan insiden keamanan dapat memiliki dampak negatif pada kepercayaan publik terhadap komunikasi publik. Ketika protokol keamanan dilanggar, orang mungkin menjadi ragu untuk membagikan informasi pribadi atau terlibat dalam komunikasi publik. Hal ini dapat berakibat pada terhambatnya komunikasi yang efektif antara pemerintah, organisasi, dan masyarakat.
Penting untuk meningkatkan kepatuhan terhadap protokol keamanan dalam komunikasi publik untuk membangun kepercayaan dan melindungi informasi sensitif. Hal ini dapat dicapai melalui edukasi dan pelatihan, pengembangan teknologi yang aman, dan penegakan protokol yang konsisten.

Protokol keamanan dalam komunikasi publik memiliki dampak positif dan negatif yang signifikan. Dampak positifnya meliputi meningkatkan keamanan data pribadi dan profesional, mengurangi risiko serangan siber, dan memastikan kerahasiaan informasi. Dampak negatifnya meliputi meningkatkan biaya operasional, menurunnya nilai transaksi melalui internet, dan merugikan secara moral dan materi bagi korban yang data-data pribadinya dimanipulasi.
Protokol keamanan dalam komunikasi publik sangat penting dalam era digital yang semakin maju. Dengan menggunakan protokol keamanan yang sesuai, seperti enkripsi email dan penggunaan jaringan Wi-Fi terenkripsi, penggunaan teknologi informasi dan komunikasi dapat dilakukan dengan lebih aman. Hal ini dapat mengurangi risiko serangan siber dan memastikan kerahasiaan informasi. Selain itu, protokol keamanan juga dapat membantu meningkatkan keamanan data pribadi dan profesional, sehingga penggunaan teknologi informasi dan komunikasi dapat dilakukan dengan lebih tenang dan aman.

Namun, protokol keamanan dalam komunikasi publik juga memiliki dampak negatif. Salah satu dampak negatifnya adalah meningkatkan biaya operasional. Dengan menggunakan protokol keamanan yang sesuai, biaya operasional dapat meningkat,

sehingga dapat menjadi beban bagi beberapa organisasi. Selain itu, protokol keamanan juga dapat menurunkan nilai transaksi melalui internet, sehingga dapat merugikan secara materi bagi beberapa organisasi. Dampak negatif lainnya adalah merugikan secara moral dan materi bagi korban yang data-data pribadinya dimanipulasi.

Protokol keamanan dalam komunikasi publik harus dibandingkan dengan best practices dan standar internasional. Best practices dan standar internasional dapat membantu meningkatkan efisiensi dan efektifitas protokol keamanan, serta mengurangi risiko serangan siber. Contohnya, best practices dan standar internasional dapat membantu meningkatkan keamanan data pribadi dan profesional, serta mengurangi risiko serangan siber.

E. KESIMPULAN

Hasil menunjukkan bahwa kepatuhan yang rendah terhadap protokol keamanan siber dapat merusak kepercayaan publik, yang sangat penting dalam konteks media penyiaran komunikasi Islam. Media ini memiliki peran strategis dalam membangun kesadaran publik tentang pentingnya keamanan informasi di era digital. Dengan meningkatkan kepatuhan melalui edukasi dan pelatihan, media penyiaran komunikasi Islam dapat berkontribusi pada peningkatan kesadaran masyarakat mengenai risiko dan tantangan yang ada.

Dampak positif dari protokol keamanan, seperti peningkatan keamanan data, juga sejalan dengan tujuan media penyiaran komunikasi Islam untuk menyediakan informasi yang aman dan dapat dipercaya. Sementara itu, dampak negatif seperti peningkatan biaya operasional dan kerugian bagi korban manipulasi data pribadi menunjukkan perlunya media untuk tidak hanya menyampaikan informasi, tetapi juga mengedukasi audiens tentang cara melindungi diri dalam dunia digital..

F. DAFTAR PUSTAKA

Andy, S., & Rahardjo, B. (2018). Keamanan Komunikasi Pada Protokol MQTT untuk Perangkat IoT. *Prosiding Seminar Nasional Teknik Elektro UIN Sunan Gunung Djati Bandung*, 176–184.

Dewi, S. (2020). Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis. *EVOLUSI: Jurnal Sains Dan Manajemen*, *8*(1).

Dewi, S. A. E. (2021). Komunikasi Publik Terkait Vaksinasi Covid 19. *Health Care: Jurnal Kesehatan*, *10*(1), 162–167.

Dugan, T., & Zou, X. (2020). A survey of secure multiparty computation protocols for privacy preserving genetic tests. *2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, 173–182.

Mujiastuti, R., & Prasetyo, I. (2021). Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE. *Prosiding Semnastek*.

Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, *32*, 17–31.

Prayama, D., & Yolanda, A. (2021). Protokol HTTPS, Apakah Benar-benar Aman? *Journal of Applied Computer Science and Technology*, *2*(1), 7–11.

Priyatna, C. C., Prastowo, F. X. A. A., Syuderajat, F., & Sani, A. (2020). Optimalisasi teknologi informasi oleh lembaga pemerintah dalam aktivitas komunikasi publik. *Jurnal Kajian Komunikasi*, *8*(1), 114–127.

Ramadani, T. (2019). Pengelolaan Komunikasi Publik. *Jurnal Good Governance*, *15*(1).

Saleh, M., Batoebara, M. U., & Kamaruzzaman, K. (2021). URGENSITAS TEKNORELIGION DALAM PESAN-PESAN AGAMA MELALUI TEKNOLOGI KOMUNIKASI. *Network Media*, *4*(1), 17–28. https://doi.org/10.46576/jnm.v4i1.1142

Susanto, Y. K., & Handayani, R. (2008). Intensitas Ancaman Keamanan Sistem Informasi Akuntansi Komputerisasian. *Jurnal Bisnis Dan Akuntansi*, *10*(3), 113–126.

Zerka, F., Barakat, S., Walsh, S., Bogowicz, M., Leijenaar, R. T. H., Jochems, A., Miraglio, B., Townend, D., & Lambin, P. (2020). Systematic review of privacy-preserving distributed machine learning from federated databases in health care. *JCO Clinical Cancer Informatics*, *4*, 184–200.