SecureSurgiNET

Iqbal, Sohail; Farooq, Shahzad; Shahzad, Khuram; Malik, Asad Waqar; Hamayun, Mian Muhammad; Hasan, Osman

DOI:
10.1177/1550147719873811

Privacy, Security and Trusted Computing for IoT based Healthcare Systems - Research Article

International Journal of Distributed Sensor Networks

International Journal of Distributed Sensor Networks
2019, Vol. 15(9)

DOI: 10.1177/1550147719873811
journals.sagepub.com/home/dsn
SAGE

SecureSurgiNET: A framework for ensuring security in telesurgery

Sohail Iqbal[1], Shahzad Farooq[1], Khuram Shahzad[1], Asad Waqar Malik[1,2], Mian M Hamayun[1,3] and Osman Hasan[1]

Abstract

The notion of surgical robotics is actively being extended to enable telesurgery, where both the surgeon and patient are remotely located and connected via a public network, which leads to many security risks. Being a safety-critical application, it is highly important to make telesurgery robust and secure against active and passive attacks. In this article, we propose the first complete framework, called SecureSurgiNET, for ensuring security in telesurgery environments. SecureSurgiNET is primarily based on a set of well-established protocols to provide a fool-proof telesurgical robotic system. For increasing the efficiency of secured telesurgery environments, the idea of a telesurgical authority is introduced that ensures the integrity, identity management, authentication policy implementation, and postoperative data security. An analysis is provided describing the security and throughput of Advanced Encryption Standard during the intraoperative phase of SecureSurgiNET. Moreover, we have tabulated the possible attacks on SecureSurgiNET along with the devised defensive measures. Finally, we also present a time complexity analysis of the SecureSurgiNET through simulations.

Keywords

Telesurgery, security, Advanced Encryption Standard, preoperative setup, robotic surgery

Date received: 24 May 2019; accepted: 4 August 2019

Handling Editor: Naveen Chilamkurti

Introduction

Robotic surgery is an emerging surgical trend that is leading to the birth of telesurgery.[1] In robotics, surgeons perform surgeries while sitting in close proximity to the patient console. On the contrary, telesurgery enables a surgeon to operate on a patient remotely via a surgical robot and a communication network between them. Telesurgical robotic systems (TRSs)[1] allow a master (surgeon console) to operate on a slave (called surgical robot) situated at a remote geographical location. The surgeon visualizes the robotic arms' response and movement through video feedback on his console and controls the robotic arms accordingly.

Operation Lindbergh was the first major breakthrough in the telesurgery domain.[2] During this operation, carried out in 2001, Marescaux and his team, based in the United States, performed robotic surgery on a patient in France using the ZEUS surgical robot. The successful accomplishment of this and many preceding telesurgical procedures paved the success of remote robotic surgery.[1,3] The success of these operations has provided the evidence that contemporary TRSs are now capable of tackling mission-critical operations in extreme environments.[1]

[1]National University of Sciences and Technology (NUST), Islamabad, Pakistan
[2]Department of Information Systems, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia
[3]University of Birmingham Dubai, Dubai, United Arab Emirates

Corresponding author:
Mian M Hamayun, National University of Sciences and Technology (NUST), Sector H-12, Islamabad 44000, Pakistan.
Email: mian.hamayun@seecs.edu.pk

Telesurgery provides numerous offerings and benefits, such as quality care to the people of underdeveloped countries, access to immediate surgical care for wounded soldiers, cost-effective solutions across geographical locations, and active intervention of remote experts in sophisticated surgeries.[4] Moreover, this technology enables expert surgeons to remotely train young surgeons all across the globe. Similarly, telesurgery can bridge the gap and inconsistencies between the healthcare systems of developing and developed countries and regions. However, all the aforementioned benefits are reliant on a secure system and its ability to support security in adversarial, uncontrolled, and hostile environments.[5] Patients' safety, security, and data privacy are some of the major obstacles and concerns in these types of procedures.[6] To the best of our knowledge, one of the main obstacles behind the widespread usage of telesurgery is the almost nonavailability of secure dedicated mechanisms for telesurgeries. To our knowledge, the Interoperable Telesurgical Protocol (ITP)[5] is the only available protocol to specifically address the security requirements of telesurgery. Although this protocol addresses the issues of authentication and confidentiality, it lacks in addressing the development and implementation of security policies in national and international environments.

The accuracy of robotic manipulations and the video feedback to the surgeon is vital for patients' safety. This accuracy is in turn mainly dependent on data integrity, which is an extremely desirable characteristic of a telesurgical system. Integrity helps in achieving the desired safety and accuracy objectives of safety-critical applications, such as telesurgery. In case of any intentional or unintentional data modification, the system must provide nonrefutable evidence to establish the chain of accountability.[7] Similarly, nonrepudiation is a key feature that provides evidence against the deniability of participating entities. Such characteristics would help in raising patients' confidence levels and thus would provide the basis for the success and widespread adoption of this telesurgical technology.[8–10]

In this article, we proposed a security framework (SecureSurgiNET) that provides a foundation for developing secure telesurgical systems. We adopt a useful classification, inspired by Dowler and Hall's[11] classification, of telesurgery for our security architecture that breaks the telesurgical procedures into three distinct phases referred to as the preoperative, intraoperative, and postoperative phases. In the preoperative phase, platform integrity is ensured. Furthermore, a secure connection between the master and slave is established based on the X.509 digital certificates and patients' biometric identities. A dummy identity is managed against a patient's real identity and is never revealed to any unauthorized entities. The authentication and authorization processes are controlled by the implementation of formal policies. Secret parameters are shared only after a successful authentication session. Similarly, SecureSurgiNET ensures encryption and authentication of communication data in both intraoperative and postoperative phases.

In the intraoperative phase, the proposed framework provides multiple Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) connections for communication. The TCP is used for reliable communication, while UDP provides throughput advantages. Moreover, Advanced Encryption Standard (AES) is used to encrypt the intraoperative phase communication, that is, video feedback from the patient to surgeon console and control commands from the surgeon to patient consoles. The proposed architecture enforces confidentiality and integrity of the data in the intraoperative phase while considering the real-time requirements. In contrast, during the postoperative phase, the postsurgical data are collected and stored securely and anonymously at the central telesurgical authority (TSA) database server (DBS) for future reference and legal requirements, if any.

In general, secure identification of doctors and patients in a telemedicine or telesurgical system is of prime importance. The key features of secure telemedicine systems include confidentiality of patient information, mutual authentication, patient anonymity, data integrity, freshness of communication, and mobility.[12] The proposed SecureSurgiNET handles the identity challenges through the use of a TSA including a strong authentication server (SAS) and an identity management server (IDMS). The TSA maintains a complete record of participating entities, including doctors and patients via the security administrator (SA) IDMS. Further details are given in section "SecureSurgiNET: the proposed framework."

The organization of this article is as follows: first, background and related work are presented. Then possible attacks and challenges to telesurgical systems are discussed, followed by details on the proposed architecture of our framework along with the design and flow of different protocols. In the following section, we discuss some results of video encryption as well as their analysis. In the end, we conclude this article and discuss potential future work.

Background and related work

Telesurgery mainly relies upon surgical robotics and communication networks, that is, Internet. After years of research in surgical robotics, ZEUS and da Vinci surgical robots are now commercially available.[3] ZEUS was also used in the first ever transatlantic surgery, known as Operation Lindbergh[13] in 2001. In this surgical procedure, Dr Marescaux and his team performed

laparoscopic cholecystectomy that is, removal of gallbladder using a minimally invasive procedure, on a 68-year-old woman at a hospital in Strasbourg, France. The doctor and his team were operating from New York, USA. The underlying network facilities were provided by France Telecommunications, which was a high-bandwidth, reliable, secure, and low-latency asynchronous transfer mode (ATM) network.[2] The ZEUS surgical robotic system was replaced by the da Vinci system, which is another teleoperated surgical robotic system and has a comparable efficiency.[14]

Regardless of the recent research advances in robotic surgery, very little progress has been made in the area of security of telesurgery. To date, there does not exist any complete security framework, specifically for designing and developing security aspects of telesurgical systems. There is a dire need for a security framework that takes into account the safety as well as legal and technical requirements of telesurgeries.[15,16] The most significant work in telesurgery so far is the development of ITP, which is designed for interoperability between the telesurgical robots and controllers.[17] But it ignores the security requirements of telesurgery.

Secure ITP is an enhancement of ITP[5] that uses the open software tools and Federal Information Processing Standards (FIPS) guidelines to develop a prototype to address the stringent telesurgery security requirements. Secure ITP addresses the four security requirements including authorization, authentication, communication, and policy development and enforcement. Secure ITP specifies two channels between the master and slave, that is, the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). TLS is used to provide security to TCP-based communication and DTLS is used for UDP communication. Secure ITP uses AES to encrypt the communication between the master and slave consoles.[5] Secure ITP is a reasonable design but fails in addressing some important issues such as patient identity theft, as well as some other administrative and legal issues.

Dowler and Hall[11] have highlighted the safety issues in telesurgery and divided the telesurgical procedures into three phases, namely preoperative, intraoperative, and postoperative phases. In another research,[18] the authors have pointed out security, availability, cost, and surgeon's legal responsibility as the major barriers in the success of remote robotic surgeries. Coble et al.[19] proposed a mechanism that allows the verifier to remotely attest the integrity of the software on a telesurgical robotic system. Tozal et al.[1] proposed a new method that integrates light-weight privacy and adaptive reliability in a single protocol, and it matches the performance of the AES cryptosystem. Bonaci et al.[20] analyzed the cybersecurity attacks against an advanced teleoperated robotic surgery system and focused on the denial-of-service (DoS) attacks. They used Fitts' law to quantify the impact and to analyze the tasks' difficulty under DoS attacks. Dong et al.[21] investigated the content modification attacks on a bilateral teleoperation system. They also proposed a safety mechanism to safeguard against a static malignant content modification attack. El Kalam et al.[22] presented a bilateral generalized predictive controller coupled to a quality of service (QoS)-friendly IP security protocol for telerobotic systems. P Fekri et al.[23] make use of machine learning algorithms to identify manipulated or incorrect commands, transmitted by any console, during a particular telesurgery. However, all of these works fail in providing a comprehensive solution to the problems related to secure telesurgery.

Besides, several remote health monitoring systems have been proposed in the literature to secure data of patients in a public network. R Amin et al.[24] proposed a multi-medical framework to ensure the anonymity and untraceability of patients during remote monitoring through sensor data. The framework also ensures confidentiality and integrity of the patient's data; however, it does not enforce security policies. V Sureshkumar et al.[25] proposed a robust communication protocol for ensuring the security of body sensor data for a smart healthcare system. The proposed system offers confidentiality, integrity, and anonymity; however, it lacks enforcement of security policies and is not fault tolerant. SD Suganthi et al.[26] proposed a light-weight authentication scheme for the IoT-enabled healthcare environments. The proposed scheme offers confidentiality and integrity; however, it overlooks anonymity and does not enforce security policies.

On the contrary, numerous generic security protocols exist which can be tailored to fulfill security requirements of telesurgery. These standardized generic protocols have well-tested security features and can be easily integrated in a variety of applications.[27] We have chosen the best security protocols and adopted the best design practices and guidelines to design a complete security framework called SecureSurgiNET. The protocols in the proposed framework provide authentication, authorization, confidentiality, integrity, anonymity, and nonrepudiation services. We argue that our proposed framework, that is, SecureSurgiNET, is the first complete setup that covers all the security requirements of the preoperative, intraoperative, and postoperative phases of any telesurgical system.

Attacks and defensive measures

Telesurgery is prone to different types of active and passive attacks. We have highlighted these attacks and countermeasures in Table 1.

Table 1. Attacks and defensive measures for TSRS.

Attack type	Instigation scenarios	Defensive measures
Eavesdropping	The attacker passively sniffs the communication and releases the sensitive patient information without permission	Encrypting the communication with secret key
Brute force attack	The attacker tries all possible keys in the key space to recover the secret key	Increasing key size that makes it computationally infeasible to try all the possible keys. The key length of more than 128 bits is considered secure
Masquerading attack	The attacker pretends to be the authorized user and tries to defeat or bypass the authentication mechanism	X.509 certificate–based strong authentication can guard against masquerading
Forgery attack	The adversary reproduces fraudulently a command and tries to play it illegitimately	Collision-resistant MAC (Message Authentication Code) provides proof against forgeries
Replay attack	The adversary illegally replays the legitimate messages/commands at a later time	Proper use of time-stamps, sequence number, and session token guards against replay attacks
Session hijacking	The attacker tries to gain unauthorized access to the surgeon/patient console by stealing or guessing the session parameters	Using the PKI to securely negotiate session parameters and use of random numbers can shun away guessing or stealing of session parameters
Viruses/worms	Viruses, worms and APTs can cause operating system malfunctions and crashes	Platform integrity verification helps early detection of such attacks
Data theft	Static and dynamic data	With proper authentication and encryption of data, theft could be avoided
Data deletion	Adversary can delete static and dynamic data	Strong authentication, authorization, and auditing help in limiting the illegal data accesses and thus provide protection against data deletion

TSRS: telesurgical robotic system; PKI: public key infrastructure; APT: advanced persistent threat.

SecureSurgiNET: the proposed framework

SecureSurgiNET is an assimilated framework and its architecture is shown in Figure 1. Security requirements of the proposed schemes are as follows: (a) security must be ensured during the preoperative, intraoperative, and postoperative phases of remote robotic surgery; (b) the scheme is designed to provide robust and time-efficient security to participating entities and assets of the telesurgical systems; (c) the postoperative phase ensures the secure record-keeping of the entire intervention with log details. The proposed SecureSurgiNET comprises a patient console (the telesurgical robot along with a computer system), a TSA with comprehensive security infrastructure, and a surgeon console (a combination of surgical robot, its control and monitoring system). The TSA security infrastructure includes an SAS, a local certification authority (LCA), an IDMS and a key distribution server (KDS), an authorization and policy server (APS), a telesurgical server (TSS), and a DBS.

The SecureSurgiNET platform uses well-established security protocols and practices for authentication, platform integrity, identity management, authorization, secure communication, and secure data storage. The following subsections discuss the proposed SecureSurgiNET architecture.

TSA

TSA is a centralized authority that acts as a trusted third-party regulatory body. All framework components must be approved and registered with the TSA. The TSA is responsible for keeping and maintaining the complete record of participating entities via the SA IDMS. The telesurgical administrator, after registration and identity management, defines the authorization policy and the level of authorization for every entity to perform various functions as per the requirement, qualification, expertise, and permissions. The following dedicated servers and components help the TSA to perform the abovementioned tasks.

The LCA server. LCA issues, verifies, revokes, and updates the X.509 standard–based digital certificates for different entities. LCA establishes a hierarchy with the higher level certification authority (CA) for further verification.

SAS. SAS ensures the authentication of participating entities, such as surgeon console, patient console, patient, and surgeons, in the preoperative phase of telesurgery. The SAS verifies certificates from the LCA and identities from IDMS for an authentication

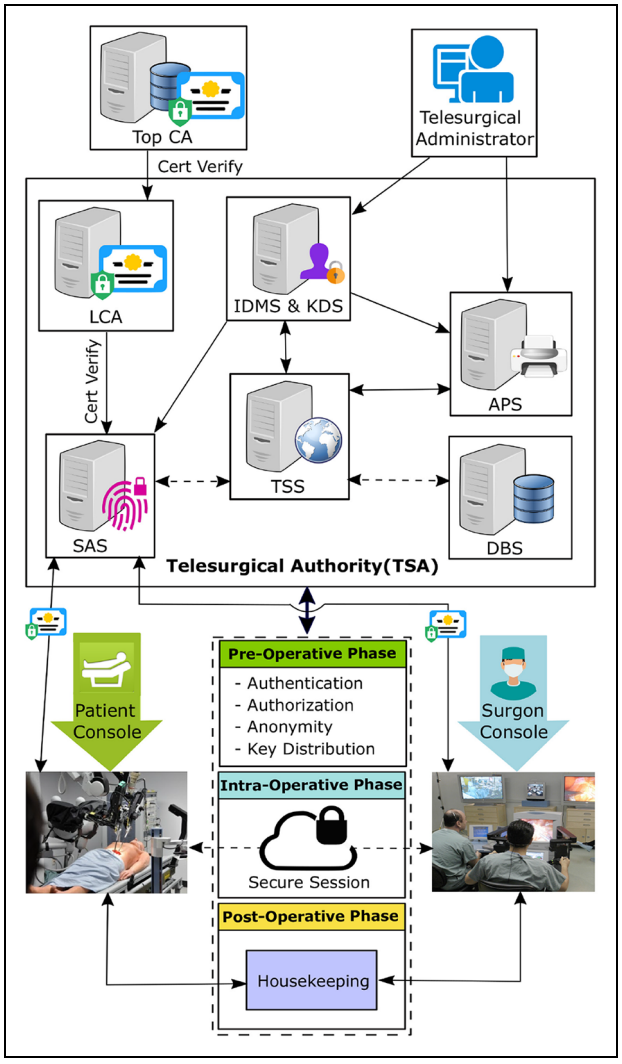

Figure 1. SecureSurgiNET framework architecture.

process. The authentication protocol proposed for our architecture is an extension of the strong authentication protocol described in FIPS-196.[28]

IDMS and KDS. IDMS is responsible for the storage and management of identities. It registers, updates, and distributes the identities for the participating entities. Furthermore, IDMS is responsible for issuing anonymous identities (AIDs) to patients against their biometric identity. These AIDs are used for protecting the patient's privacy. The KDS is liable to generate, manage, and securely distribute all the session security keys to entities.

APS. The policy server is responsible for managing the access and authorization policies. It is responsible for granting authorization to surgeons in order to conduct remote surgeries through the TSS. The TSS enforces the policies via a policy enforcement point (PEP) in coordination with its policy decision point (PDP). On successful validation of the user request, the authorization server securely issues the tokens authorizing access to the requested resources.

DBS. DBS is responsible for the secure storage of patients' medical data during the postoperative phase. An anonymous patient identity (APID) is used for data storage to protect the privacy of patients in case of any breach. Furthermore, it is ensured that access to data can only be permitted to authorized entities. The stored data are properly encrypted to ensure confidentiality and privacy of patients.

Patient console. Patient console, also known as the slave console, is appropriately equipped with the telesurgical robot, associated control, hardware/software, and the feedback devices. The feedback devices are used for providing the visual and audio feedback to the remote surgeon. This feedback is very important to judge the exact position and status of the patient and the surgical robot. All the feedback and controlling devices are registered, evaluated, and recommended by the TSA, prior to the commencement of telesurgery. Each console is embedded with a trusted platform module (TPM) chip for remote verification.

Surgeon console. Surgeon or the master console is equipped with the controlling and interacting devices to aid the surgeon to remotely control the surgical robot. The surgeon can remotely manipulate telesurgical robot on the patient console through the hardware devices and can perceive the reaction through video display. All the hardware control commands are transparently translated into communicable format and are managed by the underlying robust and secure software. The surgeon console has the TPM chip for platform integrity verification and secret key storage.

TSS. TSS interacts with different servers having TSA on behalf of authenticated users. It verifies the authenticity of users and forwards their requests to the internal resources of the TSA. It acts as a bridge between the internal and external entities. It coordinates with the TSA and sends the responses back to the users.

Design and flow of protocols

The registration phase

The TSA SA, with its administrative privileges, registers the master and slave consoles and maintains the identities in the IDMS database. The profiles of surgeons with information such as qualification, expertise, and

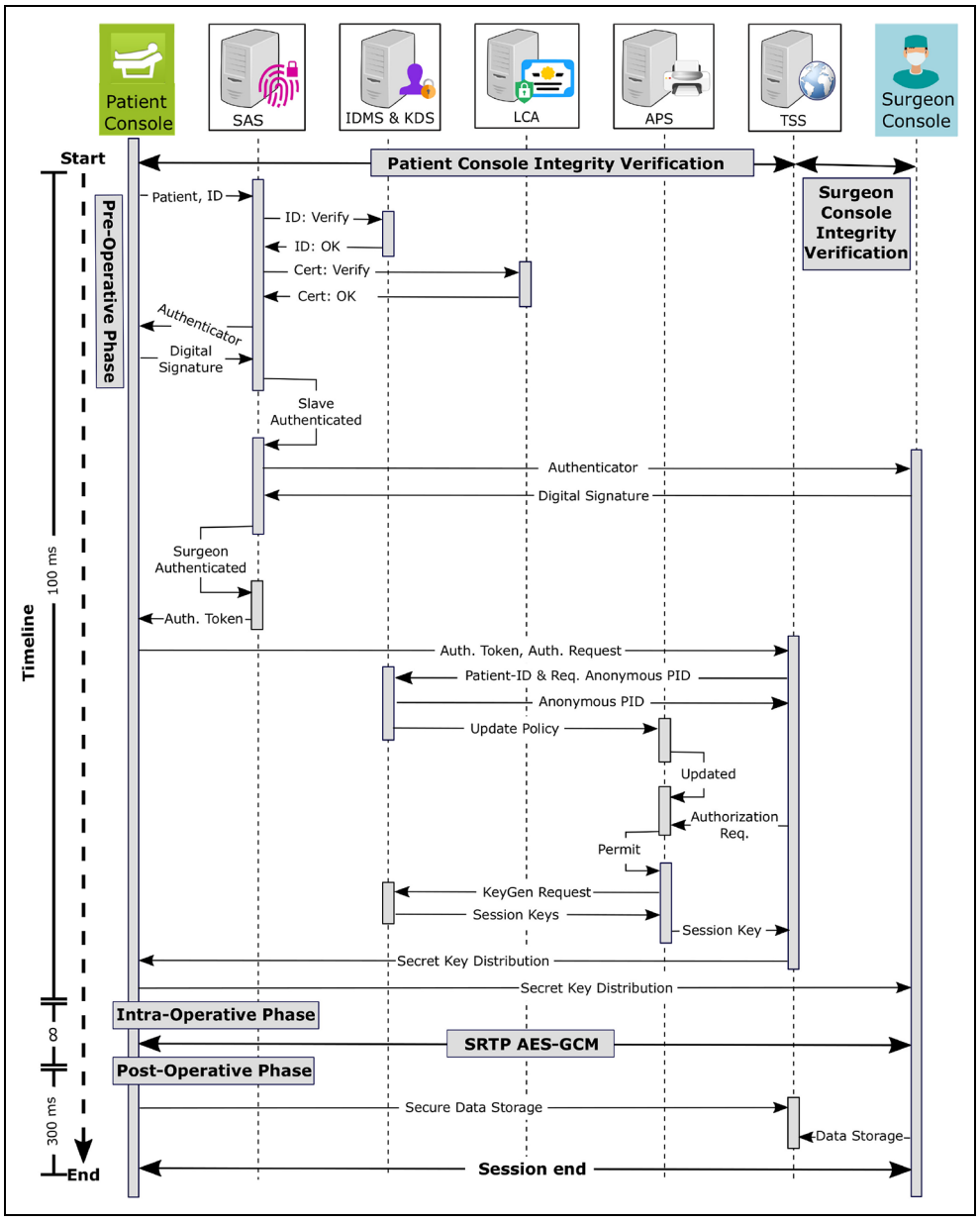

Figure 2. Protocol flow and message details of SecureSurgiNET.

capabilities are maintained in the IDMS. Policies are formulated and enforced by the SA, which also requests the LCA for the issuance of digital certificates to different entities. After the digital certificate issuance, the SA securely manages the public keys and identities in the IDMS database. All of these tasks are performed prior to the commencement of the intraoperative phase.

The flow and sequence of different protocols are shown in Figure 2. In the preoperative phase, our framework ensures platform integrity and participants' authentication, and subsequently grants authorization. In the end, the session keys are securely distributed to valid users in the preoperative phase. An AID is also issued to the patient against biometric identity in the preoperative phase. We propose to use the FIPS-196-based authentication with extended features in our framework. Digital certificates are verified by the LCA and identities are verified by the IDMS.[27]

After the successful authentication, the policy server validates and delegates authorization to perform the telesurgical procedure. During the intraoperative phase, a secure and reliable real-time protocol ensures the confidentiality and integrity of the data. TCP and UDP connections are established for reliability and throughput, respectively. AES encryption is used for confidentiality and privacy purposes. Finally, during the postoperative

phase, the complete data of the session are securely stored within the DBS against the patient's AID. This information may be used in future for postoperative follow-up.

The preoperative phase

In the preoperative phase, the platform integrity, authentication, and authorization are ensured. Patient's AID against biometric identity is also issued and maintained during this phase. Furthermore, session parameters are also negotiated in the preoperative phase. These tasks are briefly described below.

Platform integrity verification. In response to the TSA challenge, both patient and surgeon consoles calculate the platform configuration register (PCR) values and digitally sign them with the secret key embedded in the TPM chip. The PCR values are sent to the TSA for verification against the PCR values that are already stored in the TSA. If the PCR values match against the already stored values, the system is considered healthy.

Authentication process. Authentication starts with a message exchange between the slave console and the SAS. The details and format of the challenge and response messages are described in Figure 2. The TSA authenticates the patient and surgeon console on the basis of X.509 digital certificates. These certificates are verified and validated by the LCA from the issuing authority. After authentication, the TSA issues a token to get authorization.

Patient AID. After the completion of platform integrity and authentication, the next step is to generate and maintain an AID against patient's biometric identity. The TSA, after receiving the patient's biometric identity, securely issues an AID against the biometric identity. The AID adds an extra layer of protection against identity theft and enhances privacy.

Authorization process. The patient console sends an authorization request along with authentication tokens to the TSS. The TSS, after verifying the token, forwards it to the IDMS and KDS. The IDMS checks the policy against APID and sends back the response back to the TSS. After receiving the response from the IDMS, the TSS forwards the request for authorization and session key to the authorization and key distribution server. The APS, after coordinating with the policy server, permits or denies the request.

Key distribution process. If permitted, the APS requests the KDS for the session keys. The KDS generates the key for the current session and updates the IDMS database accordingly and sends the encrypted keys back to the TSS. Session keys are encrypted with the public keys of the patient and surgeon consoles. It also concatenates the session ID, random numbers, surgery type, and participants' identities with the authorization token. The KDS sends this message to authorization severs, which then in turn forward it to the TSS. The TSS passes on this message to the requesting parties, that is, patient and surgeon consoles. Patient and surgeon consoles extract the session keys and other parameters and store them securely. Now, after having the session key, they are capable of generating other keys and able to establish a secure connection based on symmetric key cryptography. This secure session ensures confidentiality and integrity of data during the intraoperative phase.

The intraoperative phase

After the completion of the preoperative phase, the intraoperative phase starts, which is very crucial for patients' safety and privacy. In this phase, patients' video data and robotic commands travel over the Internet and thus could be compromised if not properly protected. Thus, our proposed framework specifies a standard track protocol AES-GCM Authenticated Encryption in Secure Real-Time Transport Protocol (SRTP). With SRTP being a profile of a standard protocol, Real-Time Transport Protocol (RTP) is suitable for real-time audio, video, and control commands and data communication between patient and surgeon consoles. SRTP provides confidentiality, integrity, and protection against the replay attacks.

SRTP with AES-GCM can encounter computational overhead by adopting a light-weight noncryptographic hash function, called GHASH. The GHASH is a keyed hash, especially adopted for the Galois/Counter Mode (GCM) standard and adds a little overhead. Similarly, the AES provides data confidentiality in our framework. It is a standard block cipher and, as per the National Security Agency (NSA)-defined policy, it is suitable for the protection of classified and SECRET information with the key widths of 128 bits or more.[29] Moreover, it is further recommended with the key sizes of 192 and 256 bits for top SECRET communication. In the literature,[5,7] different protocols have been analyzed and AES is considered more suitable for life-critical applications.

GCM is adopted by the National Institute of Standards and Technology (NIST) as a standard for authenticated encryption and has been published in Special Publication SP-800-38D November, 2007.[30] The NIST standard provides specific implementation details for authenticated encryption. It is highlighted that GCM is efficient and accelerates the process of

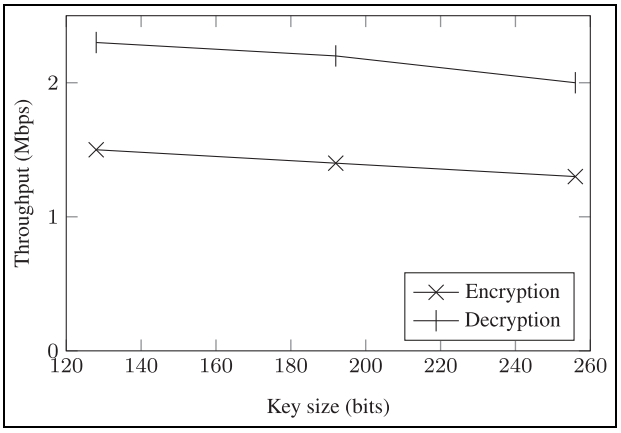

Figure 3. Comparative throughput of AES encryption and decryption for different key lengths.

authenticated encryption by providing parallel implementation in hardware as well as in software. The Intel architecture provides a specific instruction, that is, PCLMULQDQ (Carry-Less Multiplication Quadword), to accelerate performance.[31]

The postoperative phase

The postoperative phase commences once the surgical procedure is successfully completed. In this phase, both the master and slave consoles reconcile and create data backup in the DBS. The backup is stored in an encrypted form against the APID. The TSA timestamps and digitally signs the data before storing at the DBS. However, the data can be made available for different research and analysis purposes, with the permission of the patient. Furthermore, the stored data can be used for audit, in case of postsurgical complications, and to ascertain that all the responsibilities have been fulfilled. Moreover, the data can be shared with different users, such as patients, doctors, and surgeons. But, before handing over these data, these are properly formatted so that the privacy of the patients can be preserved. For this purpose, a trusted framework for health information exchange[32] is needed that makes the patient data fully unidentifiable using the l-diversity algorithm before sharing.

Results and discussion

The intraoperative phase is very crucial in terms of timely availability of patients' video data to the surgeon and transfer of control commands from the surgeon to patient console. As data encryption is a computationally intensive process, we simulate the AES for different sizes of videos to judge the performance throughput.

Table 2. SecureSurgiNET overall time delay (in ms).

	Video quality (pixels)		
AES key length (bits)	360	720	1080
128	24	48	74
192	35	77	126
256	49	104	166

AES: Advanced Encryption Standard.

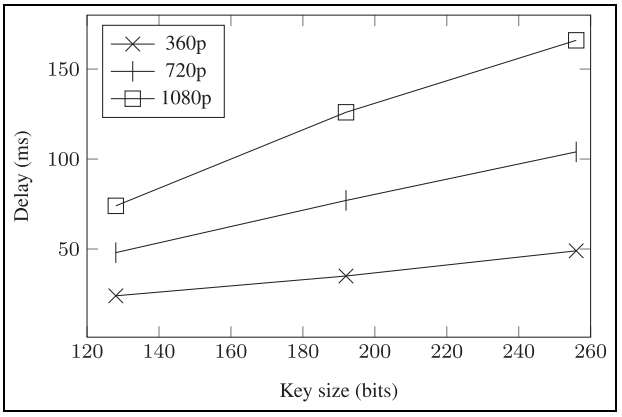

Figure 4. AES-based time delay of the SecureSurgiNET framework for different qualities of video and key lengths.

For simulation purposes, a system having a 2.40 GHz CPU, 8 GB RAM, and a Core i5 processor running Windows 8 (32 bits) and NetBeans IDE 7.4 is used. The Java cryptography classes are used to perform encryption and decryption of videos.

Results

The encryption and decryption throughputs for video files of different sizes against 128-, 192-, and 256-bit key sizes are depicted in Figure 3. The overall time delay of the SecureSurgiNET framework for different qualities of video and AES key lengths is presented in Table 2. It provides figures for the overall AES encryption time, network delay, and AES decryption time. An increase in time delay with comparatively larger key lengths can be observed from Figure 4.

Discussion

AES performance. It is evident from Figure 3 that, by increasing the key size, the throughput decreases but the level of security rises exponentially. The presented data signify that AES is quite efficient in terms of performance and higher key sizes with very minor trade-

Table 3. Comparison of SecureSurgiNET with existing approaches.

Authors	Security policies	Confidentiality	Integrity	Adaptability	Anonymity	Telesurgery	Fault tolerance	Nonrepudiation
V Sureshkumar et al.[25]	×	✓	✓	×	✓	×	×	×
SD Suganthi et al.[26]	×	✓	✓	×	×	×	×	×
R Amin et al.[24]	×	✓	✓	✓	✓	×	✓	×
P Fekri et al.[23]	×	×	×	×	×	✓	×	×
GS Lee et al.[5]	✓	×	✓	×	×	✓	×	✓
HH King et al.[17]	×	×	×	×	×	✓	×	×
SecureSurgiNET (the proposed system)	✓	✓	✓	✓	✓	✓	✓	✓

offs in the throughput. The size of the TCP and UDP packets is in bytes and AES encryption adds overhead of only a few milliseconds. A very high quality video, which requires 0.15 MB/s, can easily be encrypted and decrypted without any noticeable visual impact and additional delays. This minor overhead, on the contrary, provides a high level of security and privacy to the patient's medical records.

Furthermore, it can be examined from Figure 4 that, by increasing the key size, the time delay increases as well. The same can be examined with increasing the video quality. From the data presented in Table 2 and Figure 4, we can observe that the 128-bit encrypted transmission is approximately 50% faster than the 256-bit encryption and approximately 30% faster compared with the 192-bit encryption. It can also be observed that the performance of encryption increases with the increase in video quality.

The time complexity and throughput analysis presented above clarifies that the proposed algorithm provides good performance even with a low-end computing machine. Using a state-of-the-art computing machine, one can perform these computations very fast and with very minimal overhead. Furthermore, the preoperative and postoperative phases are flexible and the time overhead will not affect the procedure significantly.

AES security. We propose to use the AES encryption to encrypt the video and command data during the intraoperative phase. The AES is the state-of-the-art encryption algorithm with three key bit lengths, that is, 128, 192, and 256 bits. The security of AES is very high compared to DES (Data Encryption Standard), 3DES, Blowfish, RC4, and IDEA (International Data Encryption Algorithm). European Union (EU) consortium recommends AES with 128 bits as the minimum for security purposes, but it is expected that 192 or 256 bits would be a more feasible choice in the next 15–20 years. There is no known successful attack against AES but DES is susceptible to linear[33] and differential cryptanalysis.[29] Blowfish has a 64-bit block size and is not suitable for most applications. Also, there are many reported attacks[34–36] against reduced-round Blowfish. Security of the ciphers is quantified with the key length and 128-bit AES is suitable for SECRET applications, while 192- and 256-bit AES for TOP SECRET purposes. There are a number of attacks reported against RC4 such as the state recovery attack,[37] secret key recovery attack,[38] and various other attacks.[39] Thus, it is concluded that AES security is suitable for telesurgical purposes due to its strong algebraic properties and the fact that there are no reported successful attacks against it. These findings are supported from the reported analysis of different encryption algorithms such as RC4, DES, 3DES, and IDEA and it was concluded that AES is a secure, fast, and reliable algorithm in terms of security and performance.[40] Furthermore, its key lengths make brute force attack impractical with the current state-of-the-art computing machines. For hash functions, we have proposed the use of GCM, which is provably secure,[41] is very efficient as well as fast due to its hardware implementation, and is fully parallelizable.[42]

Analysis

Comparison of our proposed framework with existing approaches is presented in Table 3. We can analyze that the SecureSurgiNET is more comprehensive and complete than the existing approaches in this realm. A brief description of some features is given in the following.

Security strength

The implementation of the proposed framework is based on well-established and standardized protocols to provide a robust and secure system for telesurgery. Furthermore, using digital certificates and cryptographic nonce ensures strong authentication and guards against masquerading and replay attacks.

Implementation of appropriate policies, authorization rules, and identity management reinforces our system against session hijacking. A strong cipher like AES has the potential to thwart spying and criminal privacy violations. Moreover, the dedicated servers are used for each task and, if any server is compromised, its effects will be limited only to that single resource and the attacker cannot threaten the security of other servers. A centralized TSA makes it possible to enforce strong security policies and access rules in an international environment. Thus, standardized surgical practices can be enforced effectively in the proposed architecture. Moreover, SRTP with AES-GCM ensures the implementation of security services in real time for the underlying system. Additional chaining of patient data with AID adds an extra layer of privacy.

Scalability

The design concept of the central TSA and public key infrastructure (PKI) makes the proposed framework more scalable. Moreover, it can be extended to multiple geographic locations with tighter policies to connect patients with their desired surgeons around the globe.

Adaptability

The modular design of SecureSurgiNET provides easy integration with new protocols without any significant change. If technological advances introduce more efficient and robust security protocols, our system can adapt and integrate with them quickly and without any significant update requirements.

Fault tolerance

The modular design of SecureSurgiNET enables decentralized access to different components of the system, that is, if a server/component fails (due to any reason), then it does not stop other components from working. With load balancing between different parallel servers offering the same functionality, the system continues to work in the event of failure.

Nonrepudiation

With the security policies enforcement along with the comprehensive authentication and authorization mechanisms, the system guarantees the authenticity and effectiveness of operations between different entities.

Computation and communication overhead

Although SecureSurgiNET has some overhead in terms of communication and computation, it is comparable to the alternatives such as TLS and DTLS. Adaptation of AES-GCM makes fast authentication encryption possible and thus outshines other security algorithms. Its efficient hardware and software implementation and parallelization capability makes it more proficient. The proposed SecureSurgiNET adds more value in terms of security and safety to the telesurgical systems. However, the adaptation of AES with the parallelized version of GCM can make it further valuable.

Conclusion

The proposed SecureSurgiNET framework is designed to meet the stringent safety and security requirements of telesurgical systems in all phases. The contribution of this article is multifold. To our knowledge, it is the first complete framework for the security of telesurgical systems. In the preoperative phase, the TSA forms a special purpose PKI that provides numerous benefits such as platform integrity and participant authentication and authorization. Patients' AID adds an extra layer of privacy and guards against identity theft. During the intraoperative phase, our framework provides an efficient and secure encryption and authentication scheme. This scheme is based on standardized and well-established security protocols, which offer a high level of security and throughput.

The security, along with its modularity, makes our design flexible and adaptable. It can integrate newly available protocols quite easily and with greater flexibility, without affecting much of the underlying architecture. All policies and credentials are securely and centrally managed, thus providing the capability to enforce ever-changing policies and rules. Access to the data can only be granted after proper authentication and authorization that guards against illegal data deletions and modifications. This framework provides a foundation for developing secure and robust telesurgical systems.

In future, this framework will be formally evaluated in terms of adequacy in providing security to telesurgery. For this purpose, a complete prototype or simulation setup needs to be developed.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs

Asad W Malik https://orcid.org/0000-0003-3804-997X
Mian M Hamayun https://orcid.org/0000-0002-4800-2211

References

1. Tozal ME, Wang Y, Al-Shaer E, et al. On secure and resilient telesurgery communications over unreliable networks. In: *Proceedings of the IEEE conference on computer communications workshops (INFOCOM WKSHPS)*, Shanghai, China, 10–15 April 2011, pp.714–719. New York: IEEE.
2. Marescaux J, Leroy J, Gagner M, et al. Transatlantic robot-assisted telesurgery. *Nature* 2001; 413(6854): 379–380.
3. Elprama SA, Kilpi K, Duysburgh P, et al. Identifying barriers in telesurgery by studying current team practices in robot-assisted surgery. In: *Proceedings of the 7th international conference on pervasive computing technologies for healthcare (PervasiveHealth)*, Venice, 5–8 May 2013, pp.224–231.
4. Boonyarattaphan A, Bai Y and Chung S. A security framework for e-health service authentication and e-health data transmission. In: *Proceedings of the 9th international symposium on communications and information technology*, Icheon, South Korea, 28–30 September 2009, pp.1213–1218. New York: IEEE.
5. Lee GS and Thuraisingham B. Cyberphysical systems security applied to telesurgical robotics. *Comput Stand Interf* 2012; 34(1): 225–229.
6. Sharkey N and Sharkey A. Robotic surgery: on the cutting edge of ethics. *Computer* 2013; 46(1): 56–64.
7. Stanberry B. Legal ethical and risk issues in telemedicine. *Comput Method Progr Biomed* 2001; 64(3): 225–233.
8. Prabakar M, Diaz A, Guevara DC, et al. A study of telerobotic surgery and telementoring in space missions. In: *Proceedings of the 29th southern biomedical engineering conference (SBEC)*, Miami, FL, 3–5 May 2013, pp.155–156. New York: IEEE.
9. Smithwick M. Network options for wide-area telesurgery. *J Telemed Telecare* 1995; 1(3): 131–138.
10. Holt D, Zaidi A, Abramson J, et al. Telesurgery: advances and trends. *Univ Toronto Med J* 2004; 82(1): 52–54.
11. Dowler N and Hall CJ. Safety issues in telesurgery: summary. In: *Proceedings of the IEE colloquium on towards telesurgery*, London, 20 June 1995, pp.6/1–6/3. New York: IEEE.
12. Rezaeibagha F and Mu Y. Practical and secure telemedicine systems for user mobility. *J Biomed Inform* 2018; 78(2): 24–32.
13. Herrmann KL. Cybersurgery: the cutting edge. *Rutgers Comput Technol Law J* 2005; 32(1): 297.
14. Hubens G, Coveliers H, Balliu L, et al. A performance study comparing manual and robotically assisted laparoscopic surgery using the da Vinci system. *Surg Endoscopy Interven Technique* 2003; 17(10): 1595–1599.
15. Doarn CR and Moses GR. Overcoming barriers to wider adoption of mobile telerobotic surgery: engineering, clinical and business challenges. In: Doarn CR and Moses GR. (eds) *Surgical robotics: systems applications and visions*. New York: Springer, 2011, pp.69–102.
16. Dickens BM and Cook RJ. Legal and ethical issues in telemedicine and robotics. *Int J Gynecol Obstetric* 2006; 94(1): 73–78.
17. King HH, Tadano K, Donlin R, et al. Preliminary protocol for interoperable telesurgery. In: *Proceedings of the international conference on advanced robotics*, Munich, 22–26 June 2009, pp.1–6. New York: IEEE.
18. Challacombe B, Kavoussi L, Patriciu A, et al. Technology insight: telementoring and telesurgery in urology. *Nat Clin Pract Urol* 2006; 3(11): 611–617.
19. Coble K, Wang W, Chu B, et al. Secure software attestation for military telesurgical robot systems. In: *Proceedings of the military communications conference*, San Jose, CA, 31 October–3 November 2010, pp.965–970. New York: IEEE.
20. Bonaci T, Yan J, Herron J, et al. Experimental analysis of denial-of-service attacks on teleoperated robotic systems. In: *Proceedings of the ACM/IEEE sixth international conference on cyber-physical systems*, Seattle, WA, 14–16 April 2015, pp.11–20. New York: ACM.
21. Dong Y, Gupta N and Chopra N. On content modification attacks in bilateral teleoperation systems. In: *Proceedings of the American control conference (ACC)*, Boston, MA, 6–8 July 2016, pp.316–321. New York: IEEE.
22. El Kalam AA, Ferreira A and Kratz F. Bilateral teleoperation system using QoS and secure communication networks for telemedicine applications. *IEEE Syst J* 2016; 10(2): 709–720.
23. Fekri P, Setoodeh P, Khosravian F, et al. Towards deep secure tele-surgery. In: *Proceedings of the international conference on scientific computing (CSC)*, 2018, pp.81–86, https://csce.ucmss.com/cr/books/2018/LFS/CSREA2018/CSC4135.pdf
24. Amin R, Islam SH, Gope P, et al. Anonymity preserving and lightweight multimedical server authentication protocol for telecare medical information system. *IEEE J Biomed Health Inf* 2019; 23(4): 1749–1759.
25. Sureshkumar V, Amin R, Vijaykumar VR, et al. Robust secure communication protocol for smart healthcare system with FPGA implementation. *Future Gener Comput Syst* 2019; 100: 938–951.
26. Suganthi SD, Anitha R, Sureshkumar V, et al. End to end light weight mutual authentication scheme in IoT-based healthcare environment. *J Reliab Intell Environ* 2019; 2019: 1–11.
27. Abbasi AG and Muftic S. CryptoNET: security management protocols. In: *Proceedings of the 9th World Scientific and Engineering Academy and Society (WSEAS) international conference on data networks, communications, computers*, Faro, 3–5 November 2010, pp.15–20, http://www.wseas.us/e-library/conferences/2010/Faro/DNCOCO/DNCOCO-01.pdf

28. Camarillo DB, Krummel TM and Salisbury JK. Robotic technology in surgery: past, present, and future. *Am J Surg* 2004; 188(4): 2–15.
29. Matsui M. Linear cryptanalysis method for DES cipher. In: *Proceedings of the workshop on the theory and application of cryptographic techniques*, Lofthus, 23–27 May 1993, pp.386–397. Berlin: Springer.
30. Dworkin MJ. *Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC*. Special Publication 800–38D, 28 November 2007. Gaithersburg, MD: National Institute of Standards and Technology.
31. Jankowski K and Laurent P. Packed AES-GCM algorithm suitable for AES/PCLMULQDQ instructions. *IEEE Trans Comput* 2011; 60(1): 135–138.
32. Afzal M, Hussain M, Ahmad M, et al. Trusted framework for health information exchange. In: *Proceedings of the frontiers of information technology (FIT)*, Islamabad, Pakistan, 19–21 December 2011, pp.308–313. New York: IEEE.
33. Biham E and Shamir A. Differential cryptanalysis of DES-like cryptosystems. *J Cryptol* 1991; 4(1): 3–72.
34. Kara O and Manap C. A new class of weak keys for Blowfish. In: *Proceedings of the international workshop on fast software encryption*, Luxembourg, 26–28 March 2007, pp.167–180. New York: Springer.
35. Rijmen V. *Cryptanalysis and design of iterated block ciphers*. PhD Thesis, Katholieke Universiteit Leuven, Leuven, 1997.
36. Vaudenay S. On the weak keys of Blowfish. In: *Proceedings of the international workshop on fast software encryption*, vol. 1039, Cambridge, 21–23 February 1996, pp.27–32. New York: IEEE.
37. Maximov A and Khovratovich D. New state recovery attack on RC4. In: *Proceedings of the annual international cryptology conference*, Santa Barbara, CA, 16–20 August 2008, pp.297–316. New York: Springer.
38. Biham E and Carmeli Y. Efficient reconstruction of RC4 keys from internal states. In: *Proceedings of the international workshop on fast software encryption*, Lausanne, 10–13 February 2008, pp.270–288. New York: Springer.
39. Maitra S and Paul G. New form of permutation bias and secret key leakage in keystream bytes of RC4. In: *Proceedings of the international workshop on fast software encryption*, Lausanne, 10–13 February 2008, pp.253–269. New York: Springer.
40. Mushtaque MA. Comparative analysis on different parameters of encryption algorithms for information security. *Int J Comput Sci Eng* 2014; 2(4): 76–82.
41. Iwata T, Ohashi K and Minematsu K. Breaking and repairing GCM security proofs. In: *Proceedings of the advances in cryptology*, Santa Barbara, CA, 18–22 August 2012, pp.31–49. New York: Springer.
42. Urmonov O and Kim H. An energy-efficient fail recovery routing in TDMA MAC protocol-based wireless sensor network. *Electronics* 2018; 7(12): 444–454.