US011936691B2

(12) **United States Patent**
Faisal et al.

(10) **Patent No.: US 11,936,691 B2**
(45) **Date of Patent: Mar. 19, 2024**

(54) **SECURE CLOUD COMMUNICATION ARCHITECTURE**

(71) Applicant: **Queen's University at Kingston**, Kingston (CA)

(72) Inventors: **Md. Abu Faisal**, Kingston (CA); **Mohammad Zulkernine**, Kingston (CA)

(58) **Field of Classification Search**
CPC H04L 63/16; H04L 63/163; H04L 63/166; H04L 63/08; H04L 63/04; H04L 63/06;
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

2006/0105740 A1* 5/2006 Puranik H04W 12/30 455/410

encryption with Galois/Counter mode (GCM) crypto-

graphic hash, public key cryptography, and ephemeral key

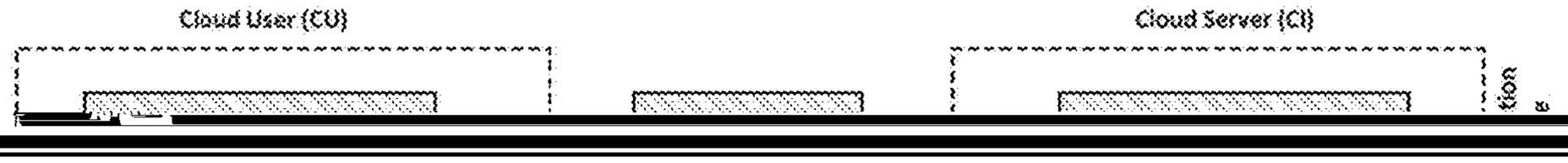
exchange, and provides faster reconnection facility for supporting frequent connectivity and dealing with connection

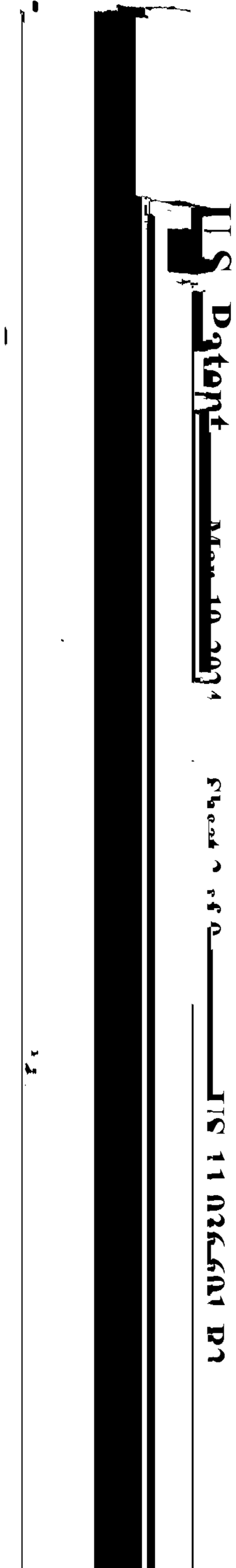
trade-offs. Embodiments have enhanced security against the above-noted attacks, and are superior to TLSv1.3 (the latest stable version among the SSL successors) in performance, bandwidth consumption, and memory usage at the server-

9/0841; H04L 9/30; H04L 9/3031; H04L 9/3236; H04L 9/3297; H04L 9/0631;
H04L 9/3247; H04L 9/0894
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS


Cloud User (CU)
Cloud Server (CS)

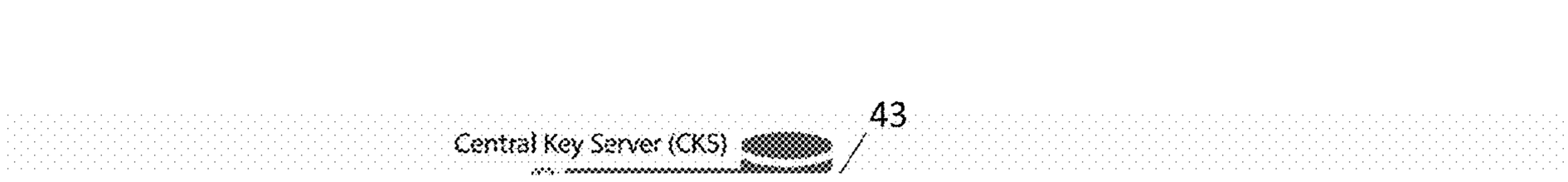


...crypt the
...ed signed
... payload

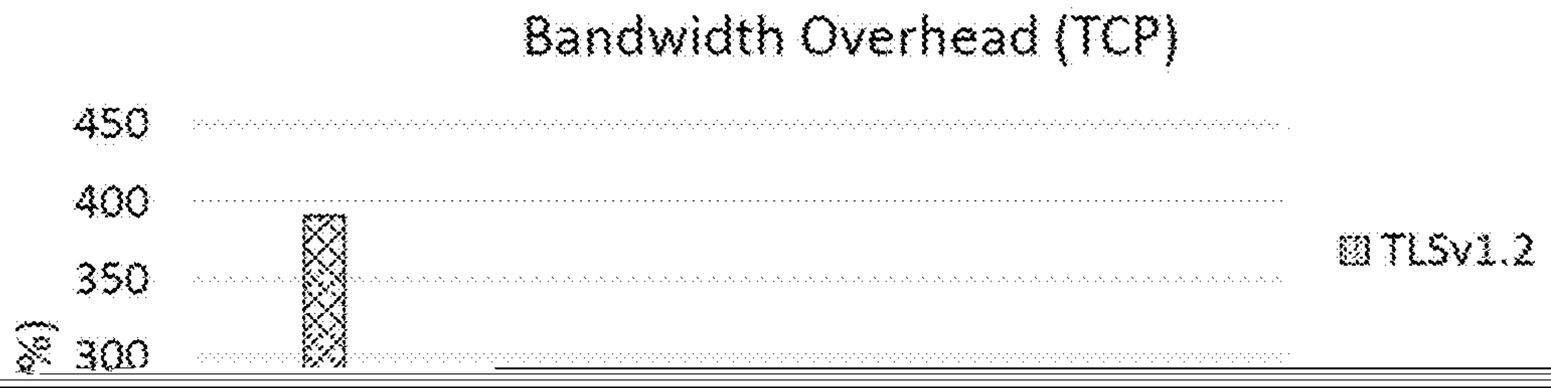
...ntiate the
...ntegrity &
...ity of the
...d payload

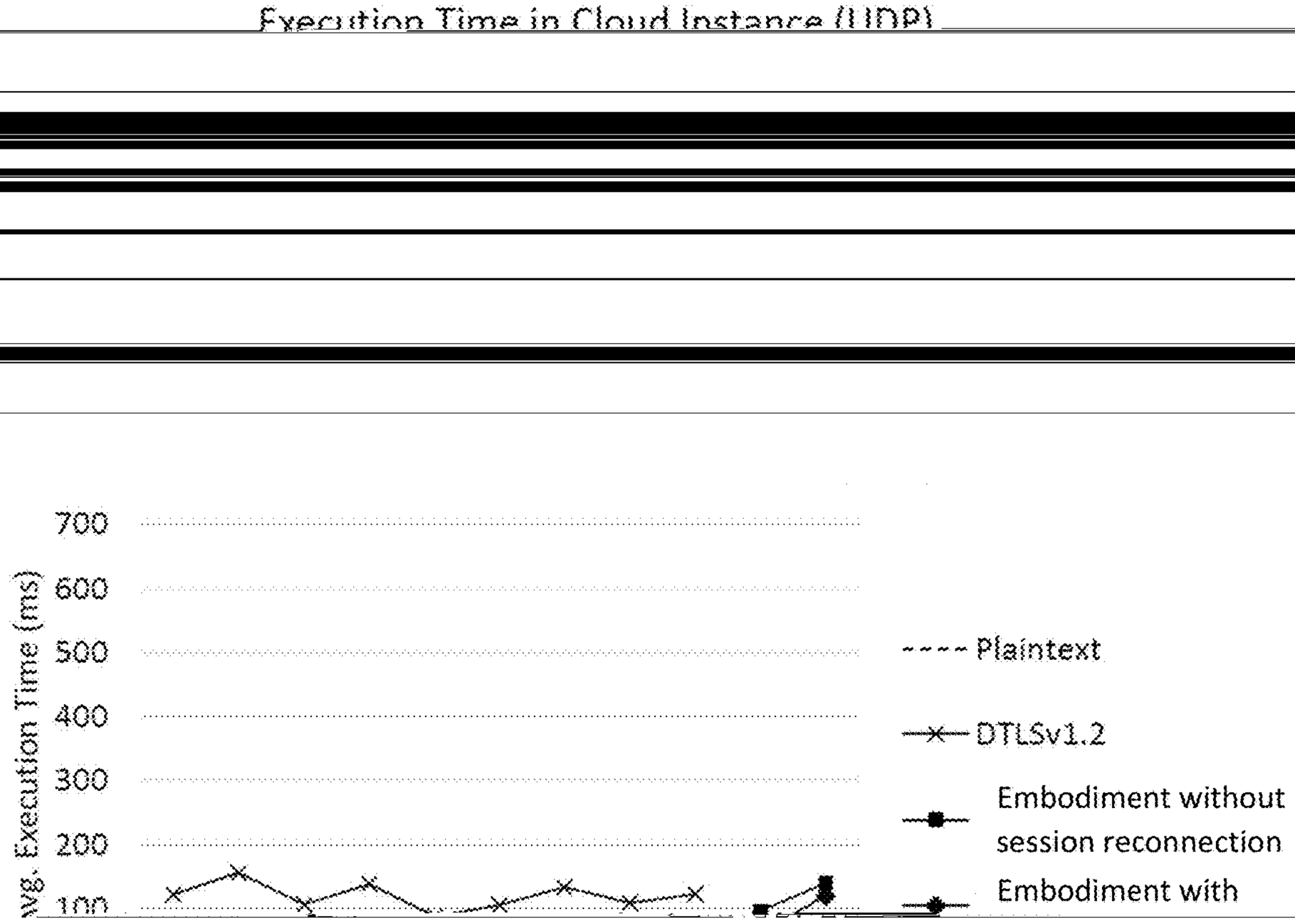
...crypt
...ntiate
...tegrity &
...y of the
...payload

...crypt
...ntiate
...tegrity &
...y of the
...payload

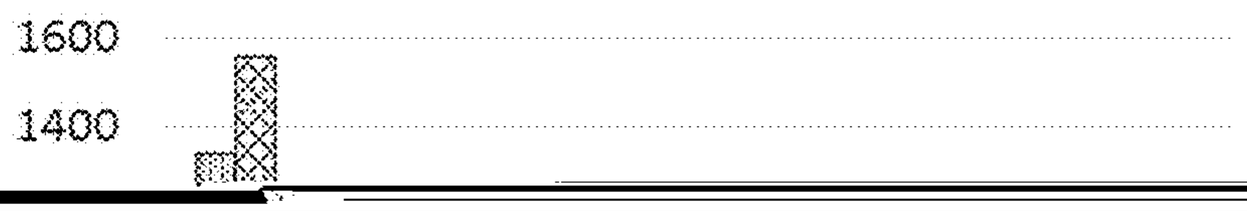

Central Key Server (CKS)
43

1200
1000
800
600
Plaintext
TLSv1.3


Bandwidth Overhead (TCP)
450
400
350
300
(%)
TLSv1.2


Execution Time in Cloud Instance (UNP)
700
600
500
400
300
200
100
Avg. Execution Time (ms)
Plaintext
DTLSv1.2
Embodiment without session reconnection
Embodiment with

[redacted]



SECURE CLOUD COMMUNICATION ARCHITECTURE

RELATED APPLICATION

This application claims the benefit of the filing date of Application No. 63/035,330, filed on Jun. 5, 2020, the contents of which are incorporated herein by reference in their entirety.

Existing traditional security protocols (e.g., SSL/TLS/DTLS) are updated from time to time. However, may still be vulnerabilities. For example, the latest version of TLS (TLSv1.3) keeps a backdoor open for middlebox compatibility. Ronen et al. [2019] showed that TLSv1.3 along with other versions of fully patched TLS implementations are prone to downgrade attack. In TLSv1.3, the first two roundtrip handshake messages are merged into a single roundtrip message to reduce the overall handshake roundtrip

[redacted]

enable embedding of other application layer communication protocols

action (encrypted request-response); wherein the CU

wherein establishing the secure cloud communications comprises the CU and the CI executing processing steps as [illegible] described in detail herein.

FIG. 2 is a sequence diagram showing the flow of execution in an architecture for TCP communications [illegible] according to one embodiment.

[illegible] execution in an architecture for UDP communications [illegible]

replay, compromised-key, repudiation, and session hijacking attacks. The results show that the embodiments efficiently mitigate these attacks, and can protect cloud communication

cation, and security is ensured for both the data and the cryptographic keys.

According to embodiments, long-term keys are not used.

In embodiments for UDP communications, message frag- [illegible]

mentation and merging, packet or sequence acknowledg- [illegible]

Termination Phase. In this phase, when the CU sends [illegible]

encrypted response back to the CU successfully, the com- [illegible]

remains valid for reconnection until it is expired.

Step-3. The cloud user (CU) connects to the cloud front- also deals with PACK messages and uses a retransmission

this connection. public-private keypair is generated. The retransmission

Step-4. The CU signs its temporary public keys with own mechanism and cryptographic hash functions are initialized

root private key to protect authenticity and integrity of the Step-2. After initialization, the CU sends a request for the

response is sent back to the CU and confirmed with a PACK message, the CI closes the datagram channel.

server (CKS) **43**, and a cloud front end (CFE) **45** connected via the internet, and cloud instances (CIs) **47***a*, **47***b*

following non-limiting Working Example.

CIs are configured according to the requirement. Each CI

gies (public key cryptography, digital signature and verification, symmetric block encryption and cryptographic hash) were evaluated iteratively for different payload sizes (100B-

eavesdropping or sniffing, thus ensuring MITM attacks cannot be successful on this type of communications.

ii) Sensitive Information Disclosure. This attack often

[redacted]

encryption technique used is prone to cryptanalysis attacks

the system. Due to the advancement of computing resources, security measures which were deemed secure in the past

reconnection (No Session) and with session-reconnection (With Session) for different payload sizes (100B, 500B, 1

plaintext attacks, compression ratio leak, discrete logarithm.

As observed from the performance curves of client-side

UDP cloud server instances. The embodiment with session-

Overall, embodiments with session-reconnection mecha-

reconnection performs about 84% faster than the DTLSv1.2

nism for both TCP and UDP communications perform

Kivinen T Kojo M · More modular exponential

(MODP) diffie-hellman groups for internet key exchange (IKE). https://tools.ietf.org/html/rfc3526

Moll R M Grance T · SP800.145 The NIST Definition s message structures selected from publish (PUB) acknowl

of Cloud Computing. http://nylpubs.nist.govinistpubs/Legacy/SP/nistspecialpublication800-145.pdf (2011).

Rescorla E · The Transport Layer Security (TLS) Proto-

5 The method of claim 1 wherein the method is implemented in a software application layer and is integrated with application protocols and server systems.

edge (ACK), reconnect (RECON), request (REQ), response (RES), expired (EXP), and error (ERR).

7 The method of claim 6 wherein the message structures

sequence-acknowledgment (SACK) message once all the MESGs in a sequence are received.

18. An apparatus including a secure cloud communication architecture for secure data in transit cloud communica-

wherein the CKS mechanism stores, revokes, and distributes root public keys securely.

20. A non-transitory computer-readable medium having

tions, comprising:

sors of two or more cloud entities of a cloud computer