Trade-off Model of Fog-Cloud Computing for Space Information Networks

Jarred Michael Carter*, **Husnu S. Narman***, **Ozlem Cosgun**†, **and Jinwei Liu**‡
* Department of Computer Sciences and Electrical Engineering, Marshall University, Huntington, WV 25755
{carter375}{narman}@marshall.edu
† Department of Information Systems Engineering & Management, Harrisburg University, Harrisburg, PA 17101
{ocosgun}@harrisburgu.edu
‡ Department of Computer and Information Sciences, Florida A&M University, Tallahassee, FL 32307
{jinwei.liu}@famu.edu

***Abstract*—A steadily growing number of Internet-based service requests from the IoT has led to an increase in complexity and number of clients, resulting in an increased number of cybersecurity concerns. Although there are main security concerns with IoT services over cloud computing services, cloud computing is mostly preferred to provide seamless and scalable Intern-based services. Moreover, cloud service providers are continuously extending their capacity to reach more industries and address their concerns. For example, Amazon has recently launched a pay-as-you-go cloud computing service that will take place on satellite operators to provide more IoT services to industries such as the agricultural and shipping industries. However, the secure transfer of information within a space information network is of great concern due to the ability of numerous attacks between nodes to occur. This can be followed by loss of data Confidentiality, Integrity, and Availability. Several researchers have proposed multifaceted solutions to these concerns, including blockchain application, digital signature, and symmetric/asymmetric encryption schemes, and centralized and/or decentralized key management for space information networks. In this paper, we focus on the integration of fog-cloud computing and space information network. We primarily investigate the feasibility of fog-cloud architecture in space information networks and the benefits of having fog computing in the security of space information networks. This is accomplished mainly by reviewing existing works on fog-cloud computing and space information networks, as well as evaluating both proposed solutions to potential issues regarding security.**

***Index Terms*—Fog Computing; space information network; trade-off**

I. Introduction

At its core, fog computing is the choice to process data wherever it is most necessary to process. In addition to facilitating all computations, storage, and networking between cloud computing data centers and networking services, architecture for this method of computing makes use of edge devices to provide an entry point into the core networks of a service provider or enterprise. Therefore, it can execute large volumes of computation, storage, and local and/or Internet-routed communicative processes.

In the traditional sense, cloud computing emerged as a business opportunity with virtualized services offered as a collection of processes within a virtual machine that can be run on large clusters of low-performance processors. In addition to a growing number of cybersecurity concerns, a steadily-growing request for Internet-based services has led to an increase in complexity and number of clients within the client/server model, resulting in a large number of cybersecurity concerns could result in loss of data Confidentiality, Integrity, and Availability.

There have been several programmatic proposals as to how this could be solved. An example is the utilization of clustered low-performance processors by programmers to enable the automated processing of data and movement operations with a simple parallel programming structure [1].

The *objective* of this paper is to investigate the existing works for eliminating and/or mitigating vulnerabilities in fog-cloud computing and space information networks, effectively allowing for the creation of a model that uses various types of layered encryption and the appropriate allocation of physical hardware for the mitigation of risks. The key *contributions* of this paper can be listed as follows:

- We first review some of the existing works in fog

computing and space information networks.
- Then, we proposed a model that integrates fog computing into space information networks.
- After that, we analyze the applicability of fog computing into the existing space information network devices.

The *results* of this paper show that the most critical issues surrounding the trade-off between fog and cloud computing involve encryption scheme, related key management schemes, and the long and variable propagation latency present due to distance between nodes in space information networks. Therefore, the proposed model can be a solution candidate to overcome the above issues.

The rest of the paper is organized as follows: In Section II, the brief background information about the related subjects is given. In Section III, the proposed model for space information network is explained. Section III also includes some of the advantages and disadvantages of integrating For Computing into Space Information Network. Section IV has the concluding remarks and our future works.

II. Background

A. Overview of Cloud Computing

Cloud computing has emerged as a method of service delivery in a pay-as-you-go manner. Various services and the related data centers are used to provide services virtually without concerning local hardware limitations. Typically, cloud computing services are dependent on load balancing, resource allocation, and efficient scheduling algorithms to coordinate the demands of all the users throughout the various geographical areas. Cloud computing services are divided into three main branches depending on the type of service. Platform as a service (PaaS) allows users to rent virtualized platforms to run their apps and services. Software as a service (SaaS) enables cloud customers to use providers' apps running on cloud infrastructure, similar to Microsoft's Office 365 services [2]. Infrastructure as a service (IaaS) provides customers with CPU usage, bandwidth, storage, and associated software that can be reconfigured as needed. There are also various types of Cloud Computing, such as Public Cloud, Private Cloud, and Hybrid Cloud that can be used to address clients' needs.

B. Overview of Fog Computing

Fog computing extends the cloud computing paradigm in one simple way: it complements cloud computing infrastructures by facilitating the creation of a hierarchical computing structure in which fog nodes play the role of an intermediary for data processing between devices and back-end data processing the cloud. This structure has evolved to include resource-poor devices in a consumer's home to powerful cloud servers, generating a tiered architecture that includes clients, fog nodes, and central servers where the bulk of processing occurs [3].

C. Overview of Risks and Vulnerabilities

Due to the nature and prevalence of cloud computing, its design ensures that it will have minimal overhead. Because fog computing inherits cloud computing traits with few added differences, the nature and prevalence of cloud computing ensure that fog computing will have minimum overhead by extension. The availability of multi-user editing in cloud computing serves as a form of support dynamic. Low latency is a consequence of fog nodes being at the edge of the network. In [4], the authors proposed solving latency issues and other related cloud computing problems by introducing an intermediate fog layer that processes communication between the cloud and end-users. In doing so, it was confirmed that fog nodes compromising the fog layer are supposed to be from different providers; it is unreasonable to trust each fog node. Cloud computing with location-based services requires the sending of location information into the cloud, resulting in privacy leaks and heavy workload pressure on the cloud itself. The performance of services can be increased by integrating machine learning techniques/algorithms [5], [6]. We further investigate security in Section III.

Issues with fog and cloud computing will negatively affect the space information network despite the pre-existing vulnerabilities of space information networks. For example, space information networks' lack of fixed infrastructure, long and variable propagation latency, high bit error rates, and high-security requirements are already challenging. Terrestrial internet protocols are rendered useless in the case of space information networks, and they must be created from scratch or re-designed and strengthened for use in the space information networks due to the high dynamics and long latency of satellites. For instance, the traditional use of TCP must evolve to overcome the inability to distinguish data losses due to link failure from network congestion, which would become a severe problem in extreme space communication environments. Long link

delays, noisy channels, and asymmetric channel rates play an important role in data loss.

Secure handoff optimization schemes for heterogeneous wireless networks must have proper Authentication, Authorization, and Accounting (AAA), which is achieved in part with a specific encryption method for this type of network. However, it is not yet possible to achieve a rapid scheme for encryption and decryption for data protection against denial-of-service, eavesdropping during signaling message transmission, and man-in-the-middle attacks. Satellite processing systems can be either singular or split. When they are not split, the processor controls its own operations, sends data, and replies to data. If a processor is compromised, adversaries will have access to both the satellite to which the processor belongs and the data being sent and/or received, which directly affects the integrity of the data; therefore, these processors must be separated. In [3], the authors highlight that authentication header protocols or encapsulating security payloads of the IPsec and internet key exchanges should be used as the Internet Engineering Task Force recommends. However, key agreements must rely on pre-shared keys or public-key authentication. Without this, IPsec cannot be deployed in space information networks without an efficient latency and signaling cost reduction method. High variable latency and a high long-link delay make the implementation of many proposed schemes complex as well.

Key management is another prominent issue in space information networks [3], [7], where the difficulty of building a powerful online key management center due to the large geographic area covered by satellites is discussed. A centralized online server in charge of key management for the generation and distribution of keys is feasible. However, it could result in transmission delay due to distance and latency and possibly be taken over in a specific geographic region due to the lack of a global perimeter and the scope of heterogeneous infrastructures that are not owned by the same party [8]. Decentralized key management would be more reliable because if one node were to become compromised, the rest of the nodes would not necessarily be affected immediately, which would give systems administrators time to respond to the system with respect to transmission delay and latency. However, with the blockchain approach proposed in [9], node storage is highly limited, which is why an asymmetric encryption scheme would cause computation costs to skyrocket due to the need for an entire blockchain to be stored on each node. Theoretically, if someone was to attempt to intercept information transfer from a fog network to a space information network, the blockchain approach would be beneficial in that it functions on one-way communication.

D. Programmatic and Algorithmic Solutions

Minimum bandwidth codes enable inverse-linear trade-off between resource consumption load and communication load by allowing for a computation load (r) increase. This reduces the required communication load for computing by the same (r) factor. In minimum latency codes, the inverse-linear trade-off is between computation load and latency, thus allowing the utilization of code for redundant computations to alleviate the effects of stragglers that slow computations by a multiplicative factor. In [4], the authors discuss the coding concepts of minimum bandwidth codes and minimum latency codes to illustrate their impacts on fog computing. A special case involving the coding concepts was elaborated on to illustrate the two codes in action. This demonstrated how coding could be used to trade abundant computing resources at the network edge for communication bandwidth and latency. Most importantly, minimum bandwidth codes reduce communication loads by a multiplicative factor of r when computing r times more subtasks than the execution without redundancy, which reduces overall response time and allows for more scalability [4]. The response time with minimum bandwidth codes is reduced to $O(logn/n)$ with maximum survivability of computations when faced with node failure or disconnection.

The usage of evolutionary algorithms has been considered by some researchers to analyze runtime and computing costs against steady-state asynchronous algorithms. In [10], the authors investigate this trade-off by performing parameter tuning experiments on instances of the Generational, Steady-State, Asynchronous, and Selection Lag evolutionary algorithms by taking a subset of solutions from tuning experiments and running them with a full Discrete-Event Simulation (DES) model on a cloud computing platform to record the runtime of data integration into a preexisting set, which is mimicked by the natural evolution-inspired design of the algorithm. The results concluded that high costs were inversely proportional to the trade-off and that high evaluations were inversely proportional to time [10]. Steady-state asynchronous algorithms have higher utilization rates but lower function evaluation efficiency than generational,

seeing that runtime decreases almost exponentially as cost increases with parallelism that is directly controlled by the offspring population size [10].

E. Other Solutions

In June 2019, NASA launched the Laser Communications Relay Demonstration [11] into geostationary orbit with a hosted payload on the US Airforce Research Lab. This was designed to complement and supersede RF single access to provide higher bandwidth duplex data links to ground or low-earth orbit users. Bandwidths ran at 2.88 Gbps when uncoded and 1.244 Gbps with the use of half-rate DVC-S2 based FEC [12]. For LCRD to provide terminal services such as relay services from NASA users in Low Earth Orbit (LEO) through Geostationary Earth Orbit to the ground stations, a terminal is required for the closure of LEO-GEO links. The Integrated Lasercomm LEO User Modem Amplifier Terminal (ILLUMA-T) is for such users and will be ready for demonstration in 2021 on the International Space Station (ISS). ILLUMA-T is equipped with a 2.88 Gbps DPSK modem with a high-power optical amplifier capable of transmitting up to 3 W at 1550 nm for communications and is able to articulate a signal over a field of regard of 360° azimuthal x 270° elevation. Success for this type of technology is heavily dependent on keeping the cost and user burden in terms of mass, size, and power comparable to that of Ka-band RF systems.

NASA's Space Communications and Navigation (SCaN) Program has also been working on 100 Gbps space and ground terminals for LEO Direct-to Earth communication. The goal with this is an extremely high bandwidth downlink at a very low cost, size, weight, and power. Current efforts are focused on satellites with 2.5 TB of memory and controllers that must be read at highly similar data rates. However, it is not designed to handle pulse-position-modulated signals from deep space missions beyond GEO because a cryogenically-cooled photon-counting receiver will not be deployed with this system [12]. Similarly, NASA's Optical PAyload for Lasercomm Science (OPALS) was installed on ISS in April 2014 to experiment with space-to-ground optical communications from LEO using a 2.5 W 1550 nm laser. A concept of operations is as follows: a telescope points to the ISS using orbital predictions without active tracking. Once the ISS rises above tree-line elevation, the flight system detects the beacon on the camera and steers the gimbal to center on it. The communications laser is then modulated with data as the pass starts, and active tracking of the beacon continues as video data is looped throughout the pass [13].

III. The Proposed Model of Space Information Network wth Fog-Cloud Capabilities

Fig. 1 shows the proposed model for Fog-cloud based Space information networks. In this model, we try to address several logistics and previous problems. The architecture of the proposed fog-based space information networks will be evaluated next year.

A. Logistics

Stream-like CTR asymmetric encryption scheme with a derivable public-key for the elimination of the need for distributing and storing keys [14] is proposed due to the impracticality of a central online key management center. ID-based cryptography for handshake duration reduction and decentralized key management [7] is implemented into this proposed encryption scheme within the makeup of a four-layer space information network complete with fog nodes spanning the terrestrial, low, medium, and geostationary earth orbits [8], [9]. Each satellite in this model contains an extra processor for its own usage, and this is not to be accessed by any other entity. Separating these processors reduces the amount of access an adversary will have in the event of one of them being compromised. An estimated cost for these processors is between $15.40 and $150 depending on the desired functionality and based on limited micro-controller prices such as Arduino prices.

A lightweight asymmetric encryption scheme suitable for space networks, the CTR encryption scheme uses a counter to ensure that there are no repetitions when generating a keystream by encrypting the counter and then adding the stream to the message in question. Key streams are generated with E(seed, public key), thus requiring the sender and the recipient to have identical keys. A nonce - a number used once - is unique and unpredictable, meaning that it is impossible to predict the next nonce in the counter. When nonces are randomly generated in a large space, the probability of collisions is kept low.

A Secure Socket Proxy for business use will be required to be present somewhere between the low-earth and medium-earth orbits of this model, and the number is dependent upon the number of satellites in the system. One proxy for every ten satellites is sufficient

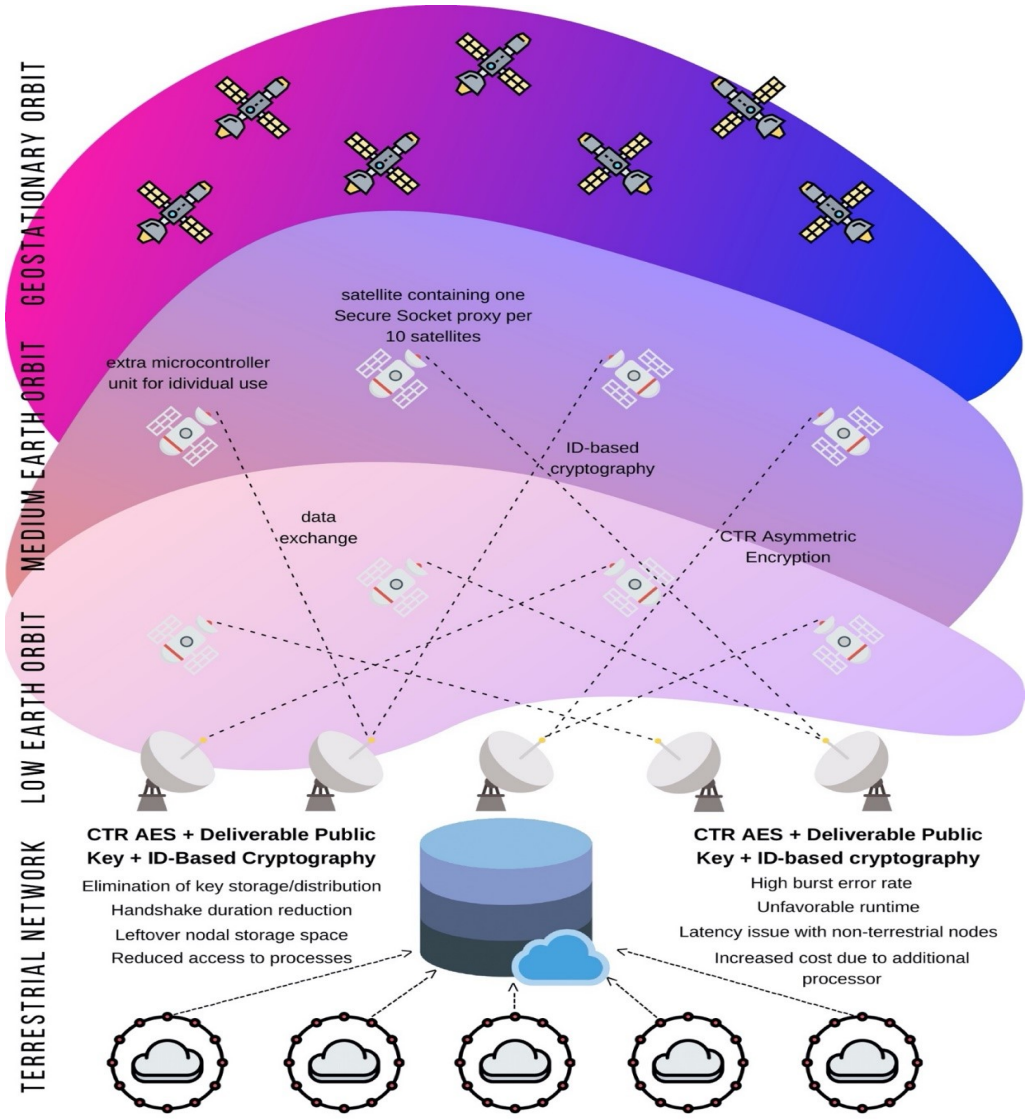

Fig. 1: The proposed model of fog-cloud computing for space information networks

enough to increase the speeds of data exchange and to preprocess. Private, dedicated proxy costs range from $81 for five to $895 for 90 [15]. Ideally, each proxy would work alongside the microcontroller units inside the satellite to ensure that the entire system is composed of satellite units equipped with fog nodes, processors, and proxies rather than deploying multiple parts into the outer atmospheres.

B. Drawbacks

Asymmetric key encryption requires that shared keys be distributed. The runtime of sharing is generally $O(n^2)$, which can be costly. Seeing that high burst errors are common among satellite communication, malicious adversaries could attempt to modify data when they detect them in addition to eavesdropping.

Propagation delays are another concern because the majority of nodes in question are not terrestrial and will be difficult to maintain in the event of an attack due to latency issues. Current systems utilizing fog computing are limited by the processing power of devices at the network edge, resulting in most data processing taking place in the cloud. Because we want the cost of a fog-computing system in a space information network to remain low, multi-core microcontroller units (MCUs) must be utilized. The architecture of multi-core MCUs allows them to stay in a deep "sleep" state when not in use and active for a short amount of time,

resulting in significantly lower power usage in terms of megawatts [16]. Homogeneous, symmetric cores would be ideal for this model to keep uniformity to a maximum among all elements of the space information network. This capacity cannot, however, be added to existing satellites. For example, if there are 800 satellites, and the total cost of new hardware is $5000 per satellite, 4 million dollars would be required to upgrade an existing network.

Quality of Service (QoS) of low latency applications (LLAs) are generally expressed as a decreasing function of each cloudlet's latency, which has the following general form:

$$u(x) = (\frac{u_{min}}{u_{max}} + (1 - \frac{u_{min}}{u_{max}})(1 - \frac{x - l_{min}}{l_{max}})^{\frac{1}{\alpha}}) * u_{max} \quad (1)$$

where u_{max} and u_{min} are representative of the maximum and minimum QoS that the application being used can have with latency l while $0 < \alpha \leq 1$. The expected quality of service (QoS) and price are directly proportional, and the cost is also directly proportional to the number of users [17].

IV. Conclusion and Future Works

In this paper, first we identify the existing problems in space information networks. In order to address those issues, a model of fog-cloud integrated space information networks is proposed. Upon the completion of the literature review and the proposed model, it was concluded that the most important issues surrounding the trade-off between fog and cloud computing involve encryption scheme, related key management schemes, and the long and variable propagation latency present due to distance between nodes and satellites. We are currently working on evaluating the proposed model for the space information networks with the explained security protocols. Further testing in a cloud simulation environment such as NS3 and/or Omnet++ is required to determine an exact runtime and a numerical estimate of the feasibility of such a fog-cloud model for space information networks.

Acknowledgments

This research was made possible by NASA West Virginia Space Grant Consortium, Training Grant # NNX15AI01H.

References

[1] N. Golpayegani and M. Halem, "Cloud computing for satellite data processing on high end compute clusters," in *IEEE International Conference on Cloud Computing*, September 21 - 25, 2009, pp. 88–92.

[2] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in fog computing: A survey," *Elsevier Future Generation Computer Systems*, vol. 88, pp. 16–27, 2018.

[3] Y. Jiang, Z. Huang, and D. H. Tsang, "Challenges and solutions in fog computing orchestration," *IEEE Network*, vol. 32, no. 3, pp. 122–129, 2017.

[4] S. Li, M. A. Maddah-Ali, and A. S. Avestimehr, "Coding for distributed fog computing," *IEEE Communications Magazine*, vol. 55, no. 4, pp. 34–40, 2017.

[5] Y. Guan, J. Shao, G. Wei, and M. Xie, "Data security and privacy in fog computing," *IEEE Network*, vol. 32, no. 5, pp. 106–111, 2018.

[6] "Data security challenges and its solutions in cloud computing," *Elsevier Procedia Computer Science*, vol. 48, pp. 204–209, 2015.

[7] C. Jiang, X. Wang, J. Wang, H.-H. Chen, and Y. Ren, "Security in space information networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 82–88, 2015.

[8] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Elsevier Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[9] *Blockchain Application in Space Information Network Security*, August 9 - 10, 2018.

[10] M. Andersson and A. H. Ng, "Parameter tuning evolutionary algorithms for runtime versus cost trade-off in a cloud computing environment," *Elsevier Simulation Modelling Practice and Theory*, vol. 89, pp. 195–205, 2018.

[11] B. L. Edwards and D. J. Israel, "Update on nasa's laser communications relay demonstration project," in *SpaceOps Conference*, 2018, p. 2395.

[12] D. M. Cornwell, "NASA's optical communications program for 2017 and beyond," in *IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, 2017, pp. 10–14.

[13] M. J. Abrahamson, B. V. Oaida, O. Sindiy, and A. Biswas, "Achieving operational two-way laser acquisition for opals payload on the international space station," in *International Society for Optics and Photonics Free-Space Laser Communication and Atmospheric Propagation XXVII*.

[14] L. Jianwei, L. Weiran, W. Qianhong, L. Dawei, and C. Shigang, "Survey on key security technologies for space information networks," *Journal of Communications and Information Networks volume*, 2016.

[15] "Plans and pricing," Trusted Proxies. [Online]. Available: https://www.trustedproxies.com/parallel-private-proxy-server-plans/

[16] M. Capra, R. Peloso, G. Masera, M. Ruo Roch, and M. Martina, "Edge computing: A survey on the hardware requirements in the internet of things world," *Multidisciplinary Digital Publishing Institute Future Internet*, vol. 11, no. 4, p. 100, 2019.

[17] A. Tasiopoulos, O. Ascigil, I. Psaras, S. Toumpis, and G. Pavlou, "Fogspot: Spot pricing for application provisioning in edge/fog computing," *IEEE Transactions on Services Computing*, 2019.