# A NOVEL SECURITY FRAMEWORK FOR CONFEDENTIALITY AND PRIVACY FOR DATA IN CLOUD BASED APPLICATIONS

**Shaik Saddam Hussian[1], Padmavathamma M[2]**
[1]PG Student, Department of Computer Science, Sri Venkateshwara University Tirupati
[2]Professor, Department of Computer Science, Sri Venkateshwara University Tirupati

**Abstract**
Cloud computing is an emerging technology as it is a multi disciplinary area. Recent news uncovers an amazing aggressor which breaks information classification by gaining cryptographic keys, by methods for intimidation or secondary passages in cryptographic programming. When the encryption key is uncovered, the main feasible measure to save information classification is to restrain the aggressor's entrance to the ciphertext. This might be accomplished, for instance, by spreading ciphertext hinders crosswise over servers in numerous authoritative spaces—accordingly expecting that the foe can't bargain all of them. By the by, if information is encoded with existing plans, an enemy outfitted with the encryption key, can in any case bargain a solitary server and decode the ciphertext squares put away in that. In this paper, we consider information secrecy against an enemy which realizes the encryption key and approaches a huge part of the ciphertext squares. To this end, we propose Bastion, a novel and proficient plan that ensures information classification regardless of whether the encryption key is spilled what's more, the foe approaches practically all ciphertext squares. We break down the security of Bastion, and we assess its execution by methods for a model usage. We additionally talk about useful bits of knowledge as for the joining of Bastion in business scattered capacity frameworks. Our assessment results recommend that Bastion is appropriate for coordination in existing frameworks since it brings about under 5% overhead contrasted with existing semantically secure encryption modes.
**Keywords:** Cloud computing, Data Confidentiality, Cryptography, Data Classification.

## I. INTRODUCTION

In real world as of late saw an enormous reconnaissance program went for breaking clients' security. Culprits were not frustrated by the different security measures conveyed inside the focused-on administrations [31].

For example, despite the fact that these administrations depended on encryption instruments to ensure information privacy, the important keying material was procured by methods for secondary passages, reward, or compulsion. On the off chance that the encryption key is uncovered, the main practical intends to ensure secrecy is to restrict the enemy's access to the ciphertext, e.g., by spreading it over different regulatory areas, in the expectation that the foe can't bargain every one of them. Nonetheless, regardless of whether the information is scrambled and scattered crosswise over various regulatory areas, a foe furnished with the suitable keying material can bargain a server in one space and unscramble ciphertext squares put away in that.

In this paper, we consider information secrecy against an enemy which realizes the encryption key and has access to an expansive portion of the ciphertext squares. The foe can gain the key either by misusing defects or then again indirect accesses in the key-age programming [31], or by bargaining the gadgets that store the keys (e.g., at the client

side or in the cloud). To the extent we are mindful, this foe discredits the security of most cryptographic arrangements, including those that ensure encryption keys by methods for mystery sharing (since these keys can be spilled when they are produced). To counter such a foe, we propose Bastion, a novel and proficient plan which guarantees that plaintext information can't be recouped as long as the foe approaches at most everything except two ciphertext squares, notwithstanding when the encryption key is uncovered. Bastion accomplishes this by consolidating the utilization of standard encryption capacities with an effective direct change. In this sense, Bastion imparts similitudes to the thought of win big or bust change. An AONT isn't an encryption independent from anyone else, yet can be utilized as a pre-handling venture before encoding the information with a square figure. This encryption worldview—called AON encryption—was mostly proposed to back off savage power assaults on the encryption key. Be that as it may, AON encryption can additionally save information privacy in the event that the encryption key is uncovered, as long as the foe approaches to at most everything except one ciphertext squares. Existing AON encryption plans, in any case, require something like two rounds of square figure encryptions on the information: one preprocessing round to make the AONT, trailed by another round for the genuine encryption. Notice that these rounds are consecutive, and can't be parallelized. This results in significant, frequently unsatisfactory, overhead to scramble and unscramble vast documents. Then again, Bastion requires just a single round of encryption which makes it appropriate to be coordinated in existing scattered capacity frameworks.

## II RELATED WORK

**"Secret-Sharing Schemes: A Survey,"**

A secret-sharing scheme is a method by which a dealer distributes shares to parties such that only authorized subsets of parties can reconstruct the secret. Secret-sharing schemes are important tools in cryptography and they are used as a building box in many secure protocols, e.g., general protocol for multiparty computation, Byzantine agreement, threshold cryptography, access control, attribute-based encryption, and generalized oblivious transfer. In this survey, we will describe the most important constructions of secret-sharing schemes, explaining the connections between secret-sharing schemes and monotone formulae and monotone span programs. The main problem with known secret-sharing schemes is the large share size: it is exponential in the number of parties. We conjecture that this is unavoidable. We will discuss the known lower bounds on the share size. These lower bounds are fairly weak and there is a big gap between the lower and upper bounds. For linear secret-sharing schemes, which is a class of schemes based on linear algebra that contains most known schemes, super-polynomial lower bounds on the share size are known. We will describe the proofs of these lower bounds. We will also present two results connecting secret-sharing schemes for a Hamiltonian access structure to the NP vs. coNP problem and to a major open problem in cryptography – constructing oblivious-transfer protocols from one-way functions.

**Using Erasure Codes Efficiently for Storage in a Distributed System**

Erasure codes provide space-optimal data redundancy to protect against data loss. A common use is to reliably store data in a distributed system, where erasure-coded data are kept in different

nodes to tolerate node failures without losing data. In this paper, we propose a new approach to maintain ensure-encoded data in a distributed system. The approach allows the use of space efficient k-of-n erasure codes where n and k are large and the overhead n-k is small. Concurrent updates and accesses to data are highly optimized: in common cases, they require no locks, no two-phase commits, and no logs of old versions of data. We evaluate our approach using an implementation and simulations for larger systems.

**Security amplification by composition: The case of doubly iterated, ideal ciphers**

One concern in using cloud storage is that the sensitive data should be confidential We investigate, in the Shannon model, the security of constructions corresponding to double and (two-key) triple DES. That is, we consider Fk1 (Fk2 ()) and Fk1 (F 1 k2 (Fk1 ())) with the component functions being ideal ciphers. This model the resistance of these constructions to \generic" attacks like meet in the middle attacks. sense. We compute a bound on the probability of breaking the double cipher as a function of the number of computations of the base cipher made, and the number of examples of the composed cipher seen, and show that the success probability is the square of that for a single key cipher. meet in the middle is the best possible generic attack against the double cipher. local revocable group signature and identity-based broadcast encryption with constant size ciphertext and private keys. To realize our concept, we equip the broadcast encryption with the dynamic ciphertext update feature, and give formal security guarantee against adaptive chosen-ciphertext decryption and update attacks.

**The security of all-or-nothing encryption: Protecting against exhaustive key search**

We investigate the all-or-nothing encryption paradigm which was introduced by Rivest as a new mode of operation for block ciphers. The paradigm involves composing an all-or-nothing transform (AONT) with an ordinary encryption mode. The goal is to have secure encryption modes with the additional property that exhaustive key-search attacks on them are slowed down by a factor equal to the number of blocks in the ciphertext. We give a new notion concerned with the privacy of keys that provably captures this key-search resistance property. We suggest a new characterization of AONTs and establish that the resulting all-or-nothing encryption paradigm yields secure encryption modes that also meet this notion of key privacy. A consequence of our new characterization is that we get more efficient ways of instantiating the all-or-nothing encryption paradigm. We describe a simple block-cipher-based AONT and prove it secure in the Shannon Model of a block cipher. We also give attacks against alternate paradigms that were believed to have the above key search resistance property.

**Deniable encryption with negligible detection probability**

Deniable encryption, introduced in 1997 by Canetti, Dwork, Naor, and Ostrovsky, guarantees that the sender or the receiver of a secret message is able to "fake" the message encrypted in a specific ciphertext in the presence of a coercing adversary, without the adversary detecting that he was not given the real message. To date, constructions are only known either for weakened variants with separate "honest" and "dishonest" encryption algorithms, or for single-algorithm schemes with non-negligible detection probability. We propose the first sender-deniable public key encryption system with a single encryption algorithm and

negligible detection probability. We describe a generic interactive construction based on a public key bit encryption scheme that has certain properties, and we give two examples of encryption schemes with these properties, one based on the quadratic residuosity assumption and the other on trapdoor permutations.

## III PROPOSED SYSTEM

In this study, we propose attacker model. We assume an adversary which can acquire all the cryptographic secret material, and can compromise a large fraction (up to all but one) of the storage servers. we addressed the problem of securing data outsourced to the cloud against an adversary which has access to the encryption key. For that purpose, we introduced a novel security definition that captures data confidentiality against the new adversary. We then proposed Bastion, a scheme which ensures the confidentiality of encrypted data even when the adversary has the encryption key, and all but *two* ciphertext blocks. Bastion is most suitable for settings where the ciphertext blocks are stored in multi-cloud storage systems. In these settings, the adversary would need to acquire the encryption key, and to compromise *all* servers, in order to recover any single block of plaintext.

## IV METHODOLOGY

We assume a computationally-bounded adversary A which *can acquire the long-term cryptographic keys used to encrypt the data.* The adversary may do so either *(i)* by leveraging flaws or backdoors in the key-generation software [31], or *(ii)* by compromising the device that stores the keys (in the cloud or at the user). Since ciphertext blocks are distributed across servers hosted

within different domains, we assume that stores the keys (in the cloud or at the user). Since ciphertext blocks are distributed across servers hosted with in different domains, we assume that the adversary cannot compromise all storage servers (cf. Figure 1).

In particular, we assume that the adversary can compromise all but one of the servers and we model this adversary by giving it access to all but $\lambda$ ciphertext blocks.

In particular, we assume that the adversary can compromise all but one of the servers and we model this adversary by giving it access to all but $\lambda$ ciphertext blocks. Note that if the adversary also learns the user's credentials to log into the storage servers and downloads all the ciphertext blocks, then no cryptographic mechanism can preserve data confidentiality. We stress that compromising the encryption key does not necessarily imply the compromise of the user's credentials. For

example, encryption can occur on a specific-purpose device [10], and the key can be leaked, e.g., by the manufacturer; in this scenario, the user's credentials to access the cloud servers are clearly not compromised.

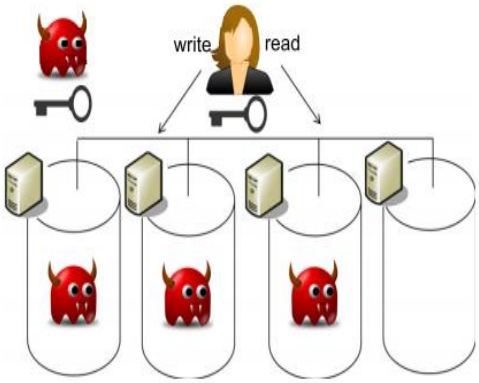


Fig: Attacker Model

## BASTION: SECURITY AGAINST KEY EXPOSURE

Bastion departs from existing AON encryption schemes. Current schemes require a pre-processing round of block cipher encryption for the AONT,

followed by another round of block cipher encryption. Differently, Bastion first encrypts the data with one round of block cipher encryption, and then applies an efficient linear post-processing to the ciphertext by doing so, Bastion relaxes the notion of all-or-nothing encryption at the benefit of increased performance.

## V CONCLUSION

In this paper, we addressed the problem of securing data outsourced to the cloud against an adversary which has access to the encryption key. For that purpose, we introduced a novel security definition that

captures data confidentiality against the new adversary. We then proposed Bastion, a scheme which ensures the confidentiality of encrypted data even when the adversary has the encryption key, and all but *two* ciphertext

blocks. Bastion is most suitable for settings where the ciphertext blocks are stored in multi-cloud storage systems. In these settings, the adversary would need to acquire the encryption key, and to compromise *all*

servers, in order to recover any single block of plaintext. We analyzed the security of Bastion and evaluated its performance in realistic settings. Bastion considerably improves (by more than 50%) the performance of existing primitives which offer comparable security under key exposure, and only incurs a negligible overhead (less than 5%) when compared to existing semantically secure encryption modes (e.g., the CTR encryption mode). Finally, we showed how Bastion can be practically integrated within existing dispersed storage systems.

## VI REFERENCES

[1] M. Abd-El-Malek, G. R. Ganger, G. R. Goodson, M. K. Reiter, and J. J. Wylie, "Fault-Scalable Byzantine Fault-Tolerant Services," in *ACM Symposium on Operating Systems Principles (SOSP)*, 2005, pp. 59–74.

[2] M. K. Aguilera, R. Janaki Raman, and L. Xu, "Using Erasure Codes Efficiently for Storage in a Distributed System," in *International Conference on Dependable Systems and Networks (DSN)*, 2005, pp. 336–345.

[3] W. Aiello, M. Bellare, G. D. Crescenzo, and R. Venkatesan, "Security amplification by composition: The case of doubly iterated, ideal ciphers," in *Advances in Cryptology (CRYPTO)*, 1998, pp. 390–407.

[4] C. Basescu, C. Cachin, I. Eyal, R. Haas, and M. Vukolic, "Robust Data Sharing with Key-value Stores," in *ACM SIGACTSIGOPS Symposium on Principles of Distributed Computing (PODC)*, 2011, pp. 221–222.

[5] A. Beimel, "Secret-sharing schemes: A survey," in *International Workshop on Coding and Cryptology (IWCC)*, 2011, pp.11–46.

[6] A. Bessani, M. Correia, B. Quaresma, F. André, and P. Sousa, "DepSky: Dependable and Secure Storage in a Cloud-of clouds," in *Sixth Conference on Computer Systems (EuroSys)*, 2011, pp. 31–46.

[7] G. R. Blakley and C. Meadows, "Security of ramp schemes," in *Advances in Cryptology (CRYPTO)*, 1984, pp. 242–268.

[8] V. Boyko, "On the Security Properties of OAEP as an All- or nothing Transform," in *Advances in Cryptology (CRYPTO)*, 1999, pp. 503–518.

[9] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable Encryption," in *Proceedings of CRYPTO*, 1997.

[10] Cavalry, "Encryption Engine Dongle," http://www.cavalrystorage.com/en2010.aspx/

[11] C. Charnes, J. Pieprzyk, and R. Safavi-Naini, "Conditionally secure secret sharing schemes with disenrollment capability," in *ACM Conference on Computer and Communications Security (CCS)*, 1994, pp. 89–95.

[12] A. Desai, "The security of all-or-nothing encryption: Protecting against exhaustive key search," in *Advances in Cryptology (CRYPTO)*, 2000, pp. 359–375.

[13] C. Dubnicki, L. Gryz, L. Heldt, M. Kaczmarczyk, W. Kilian, P. Strzelczak, J. Szczepkowski, C. Ungureanu, and M. Welnicki, "HYDRAstor: a Scalable Secondary Storage," in *USENIX Conference on File and Storage Technologies (FAST)*, 2009, pp. 197–210.

[14] M. Dürmuth and D. M. Freeman, "Deniable encryption with negligible detection probability: An interactive construction," in *EUROCRYPT*, 2011, pp. 610–626.

[15] EMC, "Transform to a Hybrid Cloud," http://www.emc. com/campaign/global/hybridcloud/index.htm.

[16] IBM, "IBM Hybrid Cloud Solution," http://www-01.ibm. com/software/tivoli/products/hybrid-cloud/.

[17] J. Kilian and P. Rogaway, "How to protect DES against exhaustive key search," in *Advances in Cryptology (CRYPTO)*, 1996, pp. 252–267.

[18] M. Klonowski, P. Kubiak, and M. Kutylowski, "Practical Deniable Encryption," in *Theory and Practice of Computer Science (SOFSEM)*, 2008, pp. 599–609.

[19] H. Krawczyk, "Secret Sharing Made Short," in *Advances in Cryptology (CRYPTO)*, 1993, pp. 136–146.

[20] J. Kubiatowicz, D. Bindel, Y. Chen, S. E. Czerwinski, P. R. Eaton, D. Geels, R. Gummadi, S. C. Rhea, H. Weatherspoon, W. Weimer, C. Wells, and B. Y. Zhao, "Ocean Store: An Architecture for Global-Scale Persistent Storage," in *International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, 2000, pp. 190–201.

[21] L. Lamport, "On inter process communication," 1985. [22] S. Micali and L. Reyzin, "Physically observable cryptography (extended abstract)," in *Theory of Cryptography Conference (TCC)*, 2004, pp. 278–296.

[23] NEC Corp., "HYDRAstor Grid Storage," http://www. hydrastor.com.

[24] M. O. Rabin, "Efficient dispersal of information for security, load balancing, and fault tolerance," *J. ACM*, vol. 36, no. 2, pp. 335–348, 1989.

[25] J. K. Resch and J. S. Plank, "AONT-RS: Blending Security and Performance in Dispersed Storage Systems," in *USENIX Conference on File and Storage Technologies (FAST)*, 2011, pp. 191–202.

[26] R. L. Rivest, "All-or-Nothing Encryption and the Package Transform," in *International Workshop on Fast Software Encryption (FSE)*, 1997, pp. 210–218.

[27] A. Shamir, "How to Share a Secret?" in *Communications of the ACM*, 1979, pp. 612–613.

[28] D. R. Stinson, "Something About All or Nothing (Transforms)," in *Designs, Codes and Cryptography*, 2001, pp. 133– 138.

[29] StorSimple, "Cloud Storage," http://www.storsimple.com/.

[30] J. H. van Lint, *Introduction to Coding Theory*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 1982.

[31] Wikipedia, "Edward Snowden," http://en.wikipedia.org/wiki/Edward_Snowden#Disclosure.

[32] Z. Wu, M. Butkiewicz, D. Perkins, E. Katz-Bassett, and H. V.Madhyastha, "SPANStore: Cost-effective Geo-replicated Storage Spanning Multiple Cloud Services," in *ACM Symposium. on Operating Systems Principles (SOSP)*, 2013, pp. 292–308.

[33] H. Xia and A. A. Chien, "RobuSTore: a Distributed Storage Architecture with Robust and High Performance," in *ACM/IEEE Conference on High Performance Networking and Computing (SC)*, 2007, p. 44.

SHAIK SADDAM HUSSIAN he is a master of Computer Science (M.Sc) pursuing in Sri Venkateswara University, Tirupati, A.P. He received Degree of Bachelor of Science in 2017 from Sri Venkateswara University, Tirupati. His research interests are Cloud Computing, Network & Security, and Big Data.