CERIAS

The Center for Education and Research in Information Assurance and Security

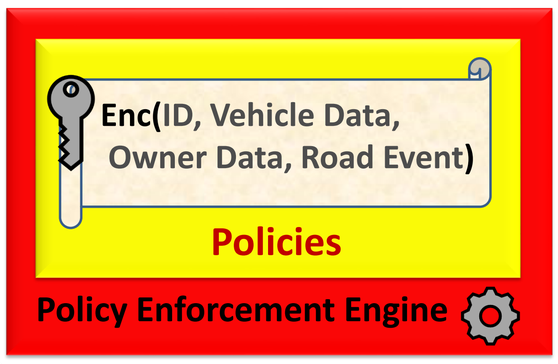
Secure Data Communication in Autonomous V2X Systems

Denis Ulybyshev[1], Aala Alsalem[1], Bharat Bhargava[1], Savvas Savvides[1], Ganapathy Mani[1], Lotfi ben Othmane[2]

[1]Computer Science and CERIAS, Purdue University; [2]Electrical and Computer Engineering Department, Iowa State University

OBJECTIVES

- Provide confidentiality and integrity of data communications in V2X systems
- Use role- and attribute-based access control for data exchanges in V2X systems
- Provide encrypted search over encrypted vehicle records



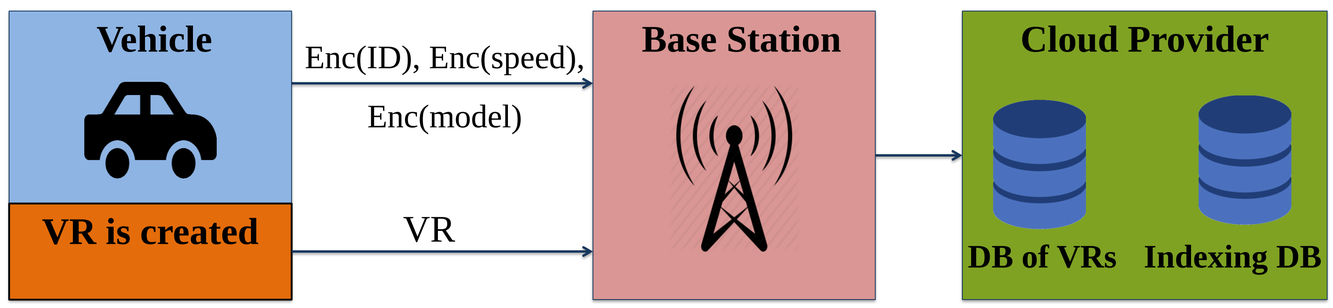
VEHICLE RECORDS

- Vehicle Records are stored in encrypted form as Active Bundles
- Created once vehicle enters base station area
- Role- and attribute-based access control for data exchange
- ID maps VR to encrypted Index DB, stored in cloud
- Embedded policy enforcement engine

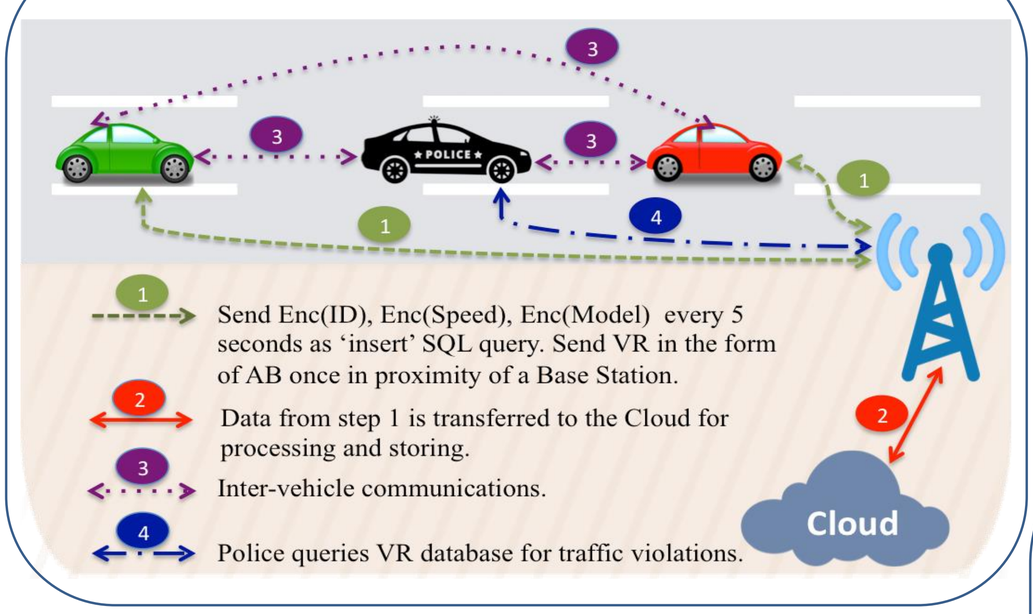
VEHICLE RECORD

VR			
ID	**Owner's Info**	**Vehicle's Info**	**Road Events**
	• Name • Address • Phone • Driver's license number	• VIN • License plate • Health Check ➢ Engine temperature ➢ Fluids Level ➢ Tires pressure	• Traffic jam • Accident • Road work • Obstacle

SYSTEM ARCHITECTURE



V2X COMMUNICATION NETWORK



ENCRYPTION SCHEMES

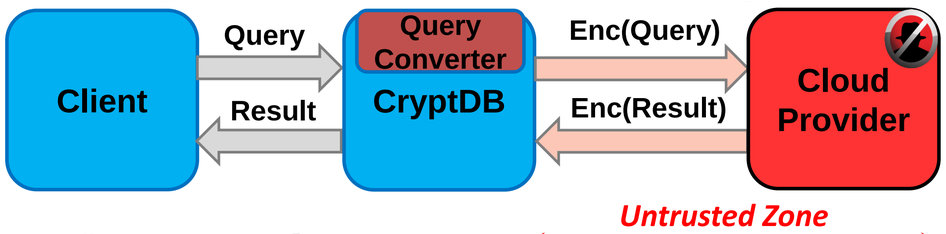
Encryption Scheme	Homomorphic Property	Supported Operations	Example
Paillier	AHE	+, SUM	Count sum of tolls paid by vehicles on a highway
ElGamal	MHE	*	Count covered distance which is multiplication: time * average speed
Boldyreva et al.	OPE	<, >, MIN, MAX	select ID, Speed, Model from IndexDB where Speed between 71 and 80
SWP	SRCH	Tokenized search	select Model from IndexDB where issue LIKE %battery%
AES	DET	Exact search	select ID, Speed from IndexDB where Model = 'Ford'

ENCRYPTED INDEXING DB

ID	Speed	Model	Timestamp
Enc(001)	Enc(65)	Enc(Toyota)	02/18/2018 15:28
Enc(002)	Enc(66)	Enc(Ford)	02/18/2018 15:29
Enc(003)	Enc(67)	Enc(Mercedes)	02/18/2018 15:31
Enc(004)	Enc(68)	Enc(Mitsubishi)	02/18/2018 15:44
⋮	⋮	⋮	⋮
Enc(1000)	Enc(84)	Enc(Chevrolet)	02/18/2018 23:59

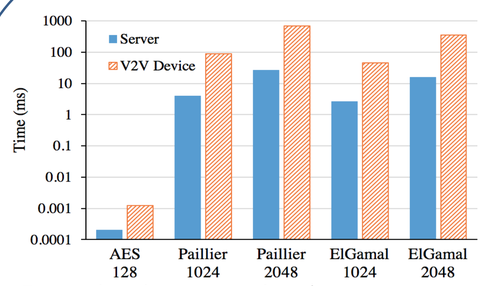
ENCRYPTED SEARCH

- Cloud provider hosts database of Vehicle Records (VRs)
- VR contains data in encrypted form
- Indexing DB has extra-attributes for indexing and search

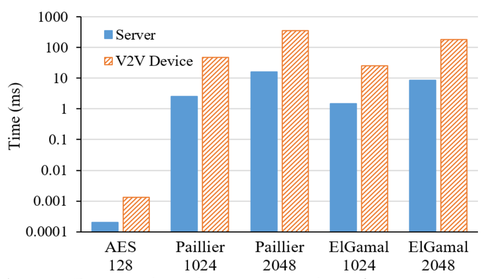


- **Query example:**
  select ID from IndexDB where speed > 76;
- **Converted query:**
  select c1 from Alias1
  where ESRCH (Enc(speed), Enc(76));

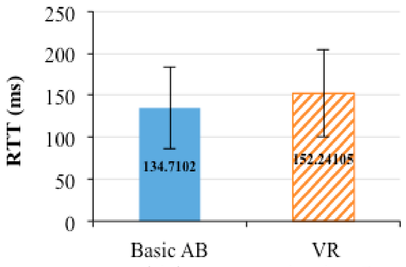
EVALUATION



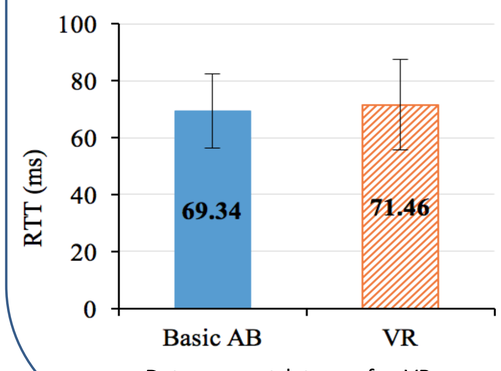
Encryption time comparison between a server and Raspberry Pi with crypto systems implemented using OpenSSL (logarithmic y-scale)



Decryption time comparison between a server and Raspberry Pi with crypto systems implemented using OpenSSL (logarithmic y-scale)

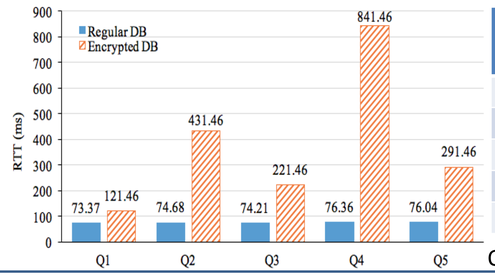


Inter-vehicle communication Round-Trip Time



Data request latency for VR, hosted by Google cloud

Equality query (Q1): SELECT ID FROM IndexDB WHERE model = Ford
Inequality query (Q2): SELECT ID,speed,model FROM IndexDB WHERE speed > 80
Inequality query, shortened (Q3): SELECT ID FROM IndexDB WHERE speed > 80
Range query (Q4): SELECT ID, speed, model FROM IndexDB WHERE speed BETWEEN 71 AND 80
Range query, shortened (Q5): SELECT ID FROM IndexDB WHERE speed BETWEEN 71 AND 80



	Query Execution Time (msec)	
	Regular Database	Encrypted Database
Q1	1.91	50
Q2	3.22	360
Q3	2.76	150
Q4	4.90	770
Q5	4.58	220

Query Execution Time

ACKNOWLEDGEMENT: This publication was made possible by NPRP grant # [7-1113-1-199] from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors. The authors would like to thank Dr. Leszek Lilien, Miguel Villarreal- Vasquez and Servio Palacios for their help and valuable feedback

PURDUE UNIVERSITY Discovery Park

CERIAS