International Institute of Information Technology Bangalore

SAMVAAD Newsletter

Theme: Cryptography and Security

August 2019

Tour de Crypto

by Prof. Bhavana Kanukurthi, Computer Science and Automation, IISc
on August 05, 2019
https://videoken.com/embed/-hRhwqTRotU
https://youtu.be/-hRhwqTRotU

Cryptanalysis of a Protocol for Efficient Sorting on Homomorphically Encrypted Data

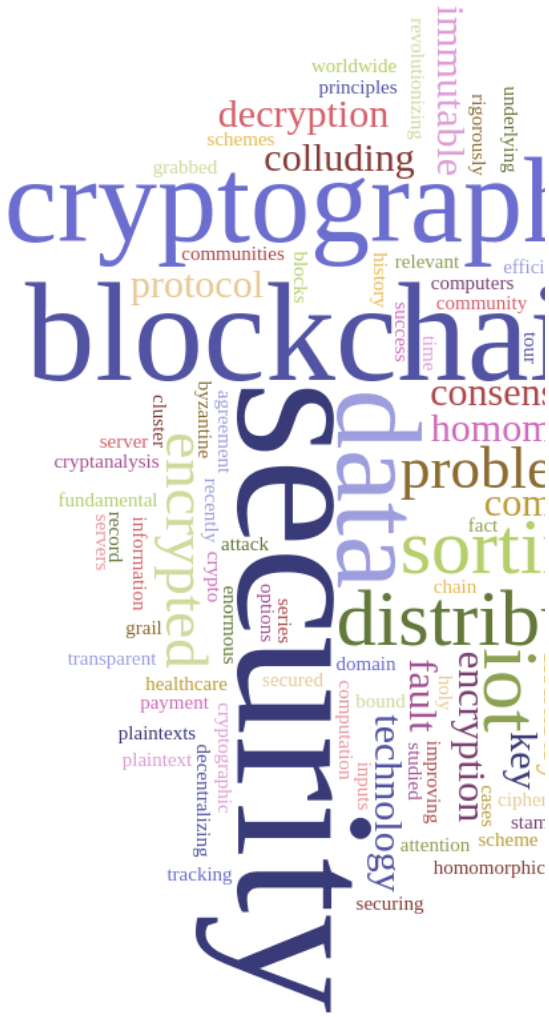
by Prof. Srinivas Vivek, IIIT Bangalore
on August 12, 2019
https://videoken.com/embed/wGEGIowB0zc
https://youtu.be/wGEGIowB0zc

Securing IoT Using Blockchain Technology

by Prof. Tricha Anjali, IIIT Bangalore
Ms. Anjana Prabhakar, IIIT Bangalore
Ms. Priti Kumari, IIIT Bangalore
On August 19, 2019
https://videoken.com/embed/-aEzJOdFJrY
https://youtu.be/-aEzJOdFJrY

Fault-tolerant Distributed Consensus: The Holy Grail Problem of Distributed Computing

by Prof. Ashish Choudhury, IIIT Bangalore
on August 26, 2019
https://videoken.com/embed/NzTrTvKviQI
https://youtu.be/NzTrTvKviQI



The theme of the Samvaad talks for the month of August 2019 was Cryptography and Security. Cryptography is a mathematical science, which deals with designing algorithms to keep sensitive data confidential, from unwanted entities. It plays a very crucial role in our day-to-day activities in the current digital age. For example, consider any kind of e-commerce application, where we want to buy things online or want to pay bills online, etc. In all these applications, we are supposed to provide our bank account details or credit card information. Cryptography helps to ensure that only the intended receiver should learn our credentials and no third party should get any kind of information about our credentials. Consider an email application, where we would like that only the intended receiver should learn our email contents and no third party should learn our email contents. Consider digital Aadhar, where an intended receiver could verify the authenticity of a digitally signed copy of the Aadhar card. In all the above examples, to ensure the security of the overall application, we use various cryptographic primitives.

As part of the Cryptography and security thematic talks, we had four speakers, who spoke about various aspects of cryptography and security. This is a summary of the talks by various speakers.

Tour de Crypto: The first talk in the series was given by Dr. Bhavana Kanukurthi, who is an assistant professor in the department of computer science and automation at the Indian Institute of Science. As the title of the talk suggests, Prof. Bhavana gave a layman's introduction to the area of cryptography and walk the audience through the wonderful and fascinating history of cryptography. In the process, she presented several simple examples, which capture the essence of this fascinating field in a very clear fashion. Various fundamental concepts like symmetric-key and asymmetric-key encryption, zero-knowledge proofs, secure computation were illustrated through illuminating examples. Towards the end, she briefly talked about her current research topics and the big open research problems in those areas. Overall, it was a very satisfying experience for the audience, who really enjoyed the talk until the end.

Data security through encryption schemes: The second talk of 'Samvaad' season took place on August 12 at IIITB campus. It was on Homomorphic encryption schemes (HE). The talk was given by Dr. Srinivas Vivek, an assistant professor at IIIT Bangalore. HE allows users to meaningfully manipulate ciphertexts without revealing any information about the underlying plaintexts. However, the talk stressed on the fact that sorting on encrypted data using HE is currently inefficient in practice when the number of elements to be sorted is very large. Hence alternate protocols that can efficiently perform computation and sorting on encrypted data are of interest.

"Recently, Kesarwani et al. (EDBT 2018) proposed a protocol for efficient sorting on data encrypted using a HE scheme in a model where one of the two non-colluding servers is holding the decryption key. In this work, Dr. Vivek and his team demonstrated an attack on the above protocol that allows the non-colluding server holding the decryption key to recover the original plaintext inputs. According to the researchers, while cryptography, which is about securing our digital data and communication, has been there for a while, Fully Homomorphic Encryption is a fairly novel concept and has application in outsourced analytics. When a plain text is encrypted, you get ciphertext. However, only those with decryption keys should be able to unlock the ciphertext. This is like putting a lock around a box and only those with a key can unlock it. Encryption schemes like HE allow computation on encrypted data. For example, we outsource our emails to Gmail instead of running the server on our own. However, Google can read all your emails to give targeted ads and this is a major privacy concern. With an efficient HE encryption scheme, while Google will not be able to read personal emails, it will still be able to throw out targeted ads.

Blockchain as future of data privacy: The third talk in the series focused on the application of blockchain in IoT (Internet of Things) industry. The session on August 19 on the IIITB campus listed some use cases and applications of blockchain and delved into its usage in the healthcare domain. The talk was given by Dr. Tricha Anjali, an associate professor at IIIT Bangalore and Ph.D. students, Ms. Anjana Prabhakar and Ms. Priti Kumari. A blockchain is a time-stamped series of immutable records of data that is managed by a cluster of computers not owned by any single entity. Each of the data block is secured and bound to one another using cryptographic principles.

The talk was on challenges that the IoT industry is facing in today's world, wherein there are many things that are getting smarter and getting connected to the internet. The IoT world has developed over several years and will continue to grow more over the coming years. Dr. Tricha explained that she and her team are focusing on various challenges that need to be sorted to make IoT more scalable. The challenges can be in terms of size, energy security, and data privacy, to mention a few. The team is working on probable solutions by implementing blockchain technology.

The session focused on data security and explored applications in healthcare. "We are looking at healthcare IoT devices, including wearable fitness devices. These devices collect personal health data constantly, which includes location, heart rate, blood pressure, sleeping pattern, etc, and it is all getting uploaded into the cloud. The company that manufactures the device has access to all the personal healthcare data of customers using these devices. A third party can purchase data from multiple such providers and put it together to get a complete picture of anyone's private life. This is a breach of privacy and a major concern in the IoT context," explained professor Tricha. The speakers articulated that a solution to these problems lies in blockchain technology. "Personal data should be available in encrypted format in the cloud and

whoever wants to access my data should meet certain conditions set by me. This can be achieved using blockchain. Various properties of blockchain technology, for instance, decentralized nature, cryptographic storage ability, immutable character, and transparent nature, make it suitable for numerous applications in the IoT industry. Use cases of blockchain in IoT are being discovered by the day, and with them, the entire system can be completely overhauled. By decentralizing the data, tracking, and improving payment options, blockchain is becoming a valuable tool for IoT, revolutionizing the industry worldwide," said Professor Tricha, during the session.

Fault-tolerant Distributed Consensus: The Holy Grail Problem of Distributed Computing: The fourth and the last talk of Samvaad focusing on 'Cryptography and Security' was held at IIITB campus on August 26. The talk was delivered by Dr. Ashish Choudhury, associate professor at IIIT Bangalore, and it revolved around the concept of 'Fault-tolerant Distributed Computing', specifically on the problem of distributed consensus. The talk began with a non-technical introduction to this area, describing the goals of a consensus protocol, the multiple settings in which the problem can be studied and various necessary conditions under which the problem can be solved. Speaking about its application in real-world problems, professor Ashish said, "Distributed consensus protocols can be useful in a variety of real-world problems, such as state-machine replication (SMR), maintaining a distributed database, etc. Ever since its inception, the consensus problem is one of the widely studied research problems, both in cryptography as well as in distributed computing community. The problem has revived interest from various other research communities, thanks to the advent and enormous success of the blockchain technology.

The session went on to discuss a particular variant of the consensus protocols, namely the class of asynchronous consensus protocols. The motivation for studying asynchronous protocols is that the real-life communication networks like the Internet are inherently asynchronous in nature, where the participating parties are non-synchronized. Dr. Ashish also spoke about the challenges faced while designing asynchronous consensus protocols. The talk ended by discussing some of the key challenging research problems in the domain of asynchronous consensus protocols.

This summary has been compiled by Dr. Ashish Choudhury, with inputs from Garima Parasher.

Credits:
Samvaad Newsletter Editors: Swathi Sharma, Jaya Sreevalsan Nair
Samvaad Video Editing and Publishing: Swathi Sharma
Photography and Video Recording: Swathi Sharma, Jay Kakkad
Technical Support: Thamarai Selvan, Vishnu Raj
Idea Conception of Samvaad Talk Series: Srinath Srinivasa
Staff Support: Director's Office, Dean's Office, Campus and Facility Management.