Homomorphic encryption

homomorphic encryption is a new technology which allows for computations on homomorphic encrypted data. this makes it easier to perform, for example, computations on highly confidential hospital or business data and allows for it to be outsourced. (because the one receiving the data doesnt know what it is and can only run computations on it without seeing the decrypted results)

Created by: 415418
Created on: October 30, 2023 1:18 PM
Changed on: October 30, 2023 2:23 PM

Context of use: Education
Level of education: Master

Technology Impact Cycle Tool

Homomorphic encryption

Impact on society

What impact is expected from your technology?

What is exactly the problem? Is it really a problem? Are you sure?

the problem is that it is momentarily unknown what the capabilities are of homomorphic encryption, we don't know what it can do, how it works, or if it's even efficient. for that reason I am performing research on this project

Are you sure that this technology is solving the RIGHT problem?

i think it is. it gives us better view of what homomorphic encryption can do and what it's capable off

How is this technology going to solve the problem?

by experimenting with the technology, we will get a better insight of how it works and what it is. as for the privacy statement made earlier: I think by encrypting data in such a way that it can be ajusted to run computations on it. you can work with confidential personal data without seeing it. making it so the privacy law has not been voided

What negative effects do you expect from this technology?

at this point in time I don't see any negative effects. the negative effects will come when someone discovers how to decrypt homomorphic encrypted data without the master encryption key

In what way is this technology contributing to a world you want to live in?

it will contribute to a more secure and privacy save world. because all data will be used without knowing to who it belongs and without seeing the original data. this means others don't know about your personal data and only about the result

Now that you have thought hard about the impact of this technology on society (by filling out the questions above), what improvements would you like to make to the technology? List them below.

if the technology could be improved in the future, it would be nice if there was an even more effective way to use it, maybe in the form of a GUI.

Hateful and criminal actors

What can bad actors do with your technology?

In which way can the technology be used to break the law or avoid the consequences of breaking the law?

This tool could be used to avoid the consequences of breaking the law. One example is the privacy law. with the help of homomorphic encryption, a company could share privacy-sensitive data so computations can be performed on it. because the data remains encrypted at all times, the person running the computations on it doesn't know what it is. making it so it doesn't void the privacy law. (only the owner of the data can decrypt the results)

Can fakers, thieves or scammers abuse the technology?

if they hjack the system and get access to this tool, they could take all the user data hostage and encrypt more data to be than sold back for a randsome or be used for blackmailing

Can the technology be used against certain (ethnic) groups or (social) classes?

yes, you could only run computation on one group and exclude the other

In which way can bad actors use this technology to pit certain groups against each other? These groups can be, but are not constrained to, ethnic, social, political or religious groups.

they can take data hostage if they gain access to a companies homomorphic encryption system and private security key

How could bad actors use this technology to subvert or attack the truth?

i dont think it could be used for that in any way. people write fake output data all the time, they dont need this tool to do that

Now that you have thought hard about how bad actors can impact this technology, what improvements would you like to make? List them below.

they should implement a more secure security encryption key system, making the system require at least 2 keys stored at different locations to decrypt the data. this way bad actors have a harder time gaining access to it

Privacy

Are you considering the privacy & personal data of the users of your technology?

Does the technology register personal data? If yes, what personal data?

it depends on how the technology is used. if you, for example, only use it for business sales computations, then no. if you use it so run computations on healthcare data of people, then yes

Do you think the technology invades the privacy of the stakeholders? If yes, in what way?

it does not, all data gets encrypted and acan only be accessed by the owner of the data. even if computations are run on it, people cant see what it is untill the owner decrypts all the data themselves

Is the technology is compliant with prevailing privacy and data protection law? Can you indicate why?

at this point in time this is not specified and a gray area, the GDPR would need to be ajusted for this technology. in my oppinion, it does follow these privacy laws though

Does the technology mitigate privacy and data protection risks/ concerns (privacy by design)? Please indicate how.

it does with the help of encryption. the whole idea of homomorphic encryption was set up to ensure private data remained private if it ever needed to be used in some kind of computation

In which way can you imagine a future impact of the collection of personal data?

the solution does create data which could follow and affect users on the longterm, but instead of infecting one person it would affect all of humanity (depending on how it is used)

Now that you have thought hard about privacy and data protection, what improvements would you like to make? List them below.

i think it should be better stated by privacy related companies how this technology fits in the privacy laws. at this time this is very vague

Human values

How does the technology affect your human values?

How is the identity of the (intended) users affected by the technology?

The identity of the user is not much affected. the computations run by this tool and encryption are something we otherwise wouldn't be able to do.

How does the technology influence the users' autonomy?

the technology makes users dependent on it for computations regarding personal and private data that can otherwise not be used or shared

What is the effect of the technology on the health and/or well-being of users?

it does not effect users in this way. unless the solution is used for computation in the healthcare sector

Now that you have thought hard about the impact of your technology on human values, what improvements would you like to make to the technology? List them below.

none atm

Stakeholders

Have you considered all stakeholders?

This category is only partial filled.

Who are the main users/targetgroups/stakeholders for this technology? Think about the intended context by answering these questions.

Name of the stakeholder
fontys lectoraat

How is this stakeholder affected?
they are the owner of the project, the ones who want to know more about encryption

Did you consult the stakeholder?
Yes

Are you going to take this stakeholder into account?
Yes

Name of the stakeholder
Casper

How is this stakeholder affected?
he is the main accessor, he will be looking into homomorphic encryption at times together with me

Did you consult the stakeholder?
Yes

Are you going to take this stakeholder into account?
Yes

Name of the stakeholder
Mark

How is this stakeholder affected?
he is an important stakeholder to which we repport progress

Did you consult the stakeholder?
Yes

Are you going to take this stakeholder into account?
Yes

Name of the stakeholder
tom broumel

How is this stakeholder affected?
project leader, all progress will be reported to him regarding the project

Did you consult the stakeholder?
Yes

Are you going to take this stakeholder into account?
Yes

Did you consider all stakeholders, even the ones that might not be a user or target group, but still might be of interest?
-

Now that you have thought hard about all stakeholders, what improvements would you like to make? List them below.
none at the moment, maybe involve a company later

Data

Is data in your technology properly used?

Are you familiar with the fundamental shortcomings and pitfalls of data and do you take this sufficiently into account in the technology?

this technollogy shouldnt be affected too much by these pitalls, as all it does is run computations on said data, therefor, it doesnt care if the data is biased or not

How does the technology organize continuous improvement when it comes to the use of data?

the technology just ingests the data and runs computations on it.

however, if the toolwas malliciously used by a hacker, they could encrypt all the data and make it unsuable for others. the program cant decide if the user is right or wrong

How will the technology keep the insights that it identifies with data sustainable over time?

N.V.T. homomorphic encryption doesnt predict any future behavior

In what way do you consider the fact that data is collected from the users?

the solution does in fact use user data in some cases for the computation. the technology doesnt profit from it though. the results comming from the computations can in some instances be shared with the owners of the data or be published online (because they do not contain the actual user data and just the result)

Now that you have thought hard about the impact of data on this technology, what improvements would you like to make? List them below.

it would be nice if there was a way to analyze the and decide how to best encrypt it and run computations on it without corrupting the data

Inclusivity

Is your technology fair for everyone?

Will everyone have access to the technology?

everyone who needs this technology can use it. at the moment it is a free technology, however, it has a steep learning curve

Does this technology have a built-in bias?

as far as i could find it does not have a built-bias. i assume it has a bias for encrypted data?

Does this technology make automatic decisions and how do you account for them?

the technology mainly depends on you for decission making, you tell it how strongly stuff must be encrypted and who has the key. all it does for you is encrypt it and generate the keys in the way that you want. these few things are not explained and i dont think there is a need to do so

Is everyone benefitting from the technology or only a a small group? Do you see this as a problem? Why/why not?

i think everyone benefits from it, because everyone has their personal information everywhere when you think about it. your bank, the hospital, the newspaper, etc. homomorphic encryption makes it so all this data can be used securely without the company having to know what this data is

Does the team that creates the technology represent the diversity of our society?

these teams are very diverse, the team that has made homomorphic encryption consist of multiple people from a lot of different backgrounds over the last 20 or so years, and it all started with just an idea of a technology

Now that you have thought hard about the inclusivity of the technology, what improvements would you like to make? List them below.

it would be nice if there was an explanation for the people so they too could understand how they would benefit from it

Transparency

Are you transparent about how your technology works?

Is it explained to the users/stakeholders how the technology works and how the business model works?

it is not easy for users to understand how homomorphic encryption works. this would require an incept workshop on homomorphic encryption and how it functions

If the technology makes an (algorithmic) decision, is it explained to the users/stakeholders how the decision was reached?

not exactly, this would require a in-depth understanding of calculus and other mathematic formulas that most people do not understand.

Is it possible to file a complaint or ask questions/get answers about this technology?

that depends on which homomorphic encryption tool you decide to use. at this point in time it's not very easy to reach those companies for questions, as the projects are still in their early days

Is the technology (company) clear about possible negative consequences or shortcomings of the technology?

yes they are, if incidents or exploits have been found regarding the solution, they will iimmediatly be posted online with a warning and the internal teams will start on looking for a solution

Now that you have thought hard about the transparency of this technology, what improvements would you like to make? List them below.

i don't think any improvements need to be made. they are very transparent regarding how the complicated formulas work but not too transparent. because you are using with encryption you can't just tell exactly how it works. because then people will miss-use that information

Sustainability

Is your technology environmentally sustainable?

In what way is the direct and indirect energy use of this technology taken into account?

improvements are possible to make the product run as efficient as possible. in theory you could create multiple pre-made script so a user would only have to do a few adjustments in the code and then run it. energy consumption wise it depends on how big and long the computation is. cutting up computations in multiple parts often results in more energy efficiency

Do you think alternative materials could have been considered in the technology?

i dont think so? the system runs on a basic computer and there isnt really anything to change

Do you think the lifespan of the technology is realistic?

i think it is, the technology keeps improving with each day. and they keep making it more and more secure. in my opinion it will at least outlive me before it gets replaced. all libraries will keep being updated and adjusted for a very long time

What is the hidden impact of the technology in the whole chain?

after the user is done with using the technology nothing happens. it just sits there and the tools subscription can be stopped. there is no need to break down or destroy any expansive machines. all it would have cost is a lot of time, which in turn would have cost manpower and energy

Now that you have thought hard about the sustainability of this technology, what improvements would you like to make? List them below.

there are no improvements i can think off at this point in time

Future

Did you consider future impact?

What could possibly happen with this technology in the future?

i think the technology could be widely used by governments and hospitals to run computations on otherwise to confidential personal data. this will help medical instances to better understand their patients and illnesses

Sketch a or some future scenario (s) (20-50 years up front) regarding the technology with the help of storytelling. Start with at least one utopian scenario.

in 10 years homomorphic encryption might take over the world. companies working with private and personal data in a secure way which allows for computations that were not able to be performed in the past because of personal data boundaries. because the technology has been getting safer and safer it is impossible for outsiders to decrypt the data. making it so that the privacy law cant be voided. in the years after, probably 20 years later. more encryption libraries and methods have been found. creating a dozen of homomorphic encryption types to be used, each with their own use and efficiency. one will be used just for IOT, the others just for the encryption and computations of persona data, etc and it will only keep growing in the future

Sketch a or some future scenario (s) (20-50 years up front) regarding the technology with the help of storytelling. Start with at least one dystopian scenario.

in a 10 homomorphic encryption might take over the world. companies working with private and personal data in a secure way which allows for computations that were not able to be performed in the past because of personal data boundaries. because the technology has been getting safer and safer it is impossible for outsiders to decrypt the data. making it so that the privacy law cant be voided. in the years after, probably 20 years later. more encryption libraries and methods have been found. creating a dozen of homomorphic encryption types to be used, each with their own use and efficiency. one will be used just for IOT, the others just for the encryption and computations of persona data, etc and it will only keep growing in the fu

Would you like to live in one of this scenario's? Why? Why not?

i wouldn't mind in living in the scenario above. usually i wouldn't want people to use and work with my personal data, but in some scenarios it has to be used, like when developing a medical cure for a new illness or to see how many people can resist a certain virus.

luckily, with homomorphic encryption the data can be used without people

seeing my data, making it so that my privacy remains in tact

What happens if the technology (which you have thought of as ethically well-considered) is bought or taken over by another party?

if the technology were to be taken over by an evil party, all hell would break lose. lets say a hospital uses it and a hacker somehow gets into the system and obtains the secure key, this would make them able to see all the data decrypted (as long as they can find all the data and know how to use the tool)

Impact Improvement: Now that you have thought hard about the future impact of the technology, what improvements would you like to make? List them below.

there is one big improvement i would like to make. the encryption system needs to be more secure. there needs to be more than just 1 secure key to decrypt the data. that way it's harder for a hacker to gain access to the key and decrypt all data