International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 12 | Dec 2021 www.irjet.net p-ISSN: 2395-0072

ANALYSIS ON PRIVACY PRESERVATION FOR THE DATA GENERATED FROM VARIOUS SOURCES USING SECURE MULTI PARTY COMPUTATION PROTOCOLS

Sai Arjun Madikonda[1]

[1]*B.Tech, Gitam Deemed to be University Hyderabad*

***

ABSTRACT : Individual wealth, financial position, and health data is highly secret, and a particular system is needed to protect these details. The appropriate input from authorized users is essential for the advancement of research and development. Even if it is in the best interests of both parties, getting sensitive information from people is extremely difficult because of concerns about their privacy. For high-quality research, getting real-time data from actual consumers is a necessity. When personal information is at stake, participants in a collaborative computation are reluctant to answer questions truthfully. The goal of secure multi-party computations is to work together to solve a variety of problems. Multiple perspectives are needed, but each one is concerned with the quality of their own contribution. All participants can keep private information about individuals or organisations safe from other participants as well as computing authorities in a secure sum problem that is currently being worked on (TTP). This research presents procedures that enhance the security, confidentiality, and anonymity of collaborative computations.

1. INTRODUCTION

Data availability has grown exponentially over the previous few decades, raising a slew of legal and privacy issues. As the use of cyberspace and its applications in e-commerce and social networking grows, adequate data preservation is vital. This scenario necessitates the development of numerous algorithms, which have been documented in the literature. Various online applications face increasing hurdles in terms of protecting user privacy and security.

Security and confidentiality are sometimes viewed as one and the same, yet they are in fact distinct concepts. Basically, security means that access to data is restricted and protected from unauthorised access. Confidentiality is ensured. Confidentiality cannot be guaranteed without adequate security. Confidentiality is concerned with ensuring that only authorized individuals have access to sensitive personal data and preventing hostile participants from accessing and calculating it.

There is a massive amount of information available online because of the rise in digitalization. This is a serious issue that warrants attention on the part of policymakers and business leaders alike. One of the most pressing concerns in collaborative computation is ensuring that information and identities remain private and anonymous. Control over the information is lost once it is shared, and it might be exploited or utilized against the party's interests by an unauthorised third party. Those outcomes that can only be gleaned from the result and what each participant has contributed are known as "secure" or "confidential."

1.1 NEED OF CONFIDENTIALITY AND SECURITY

The amount of data flowing in and out of the system has surpassed the point of no return because to digitization. For an unspecified period of time, these data are stored in repositories. Health, money, and/or business may all be impacted by this data. Because firms have a variety of reasons to secure their customers' private information, this issue is relevant. For example, a person may choose to keep his genetic health record private because releasing it could lead to social neglect.

Emotional or personal outages may occur if this material is made available online in plain language. As a result, the data must be kept private and safe.

1.2 MULTI-PARTY COMPUTATION ENVIRONMENT

Various parties on a network want to perform the same operation on the same function in multiparty computations. A PDA, a laptop, a desktop, or any other input device that is linked to the network could be one of these parties. An example of a network is a system that processes input from multiple files, an intranet that links systems, or the global internet.

1.3 SECURE MULTI-PARTY COMPUTATIONS

For example, with SMC, multiple parties can collaborate on the same private data while still ensuring the confidentiality of their information. SMC adds a new level of cooperative computation for the benefit of everybody involved. Using SMC (Dorothy, 1979; Sheikh, 2010a), participants' personal inputs are protected from disclosure by multiple individuals working together to perform computations on the secret data they provide. Individual data secrecy and safe collaborative computation are becoming increasingly important in an age of increased sociability, increased Internet use, and a massive increase in wired transactions. Collaboration in computations for mutual benefit is usually requested, but there is also concern about the privacy of individual input. It's because there's less trust in participating and computing entities.

2. LITERATURE REVIEW

P.Yoganandhini, 2020, Secure multiparty computation (SMC) based concerns are addressed in this work. Using data from three different food stores, the computation is carried out. Under Association Rule Mining, rules are generated using the FP-Tree technique to ensure anonymity (ARM). SMC's most critical criteria are confidentiality and accuracy. The items that aren't necessary in privacy requirements aren't taught. To put it another way, the parties will only be able to learn from the product. To ensure correctness, each party must receive the same output. Secure auctions employing SMC are used in this study, and frequent item sets are generated for association rule mining. Prior space complexity and subsequent time complexity are two of the most common FP-growth shortfalls." In order to improve the algorithms' performance, it was necessary to combine the FP-tree structure of the FP-growth algorithm and the Apriori algorithm. There is no continuous generation of the conditional and sub-conditional patterns in APFT.

Dankar FK, 2018, In the past, researchers would remove any identifying information, such as names and ID cards, before sharing their data with one other. However, this practise is no longer necessary. However, recent studies have shown that previously considered anonymous clinical data can be used to identify the names of research participants. Those with Alzheimer's or schizophrenia (and their blood relatives) can benefit from DNA sequencing because the genome is unique to each person and can be used to predict future health issues (such as Alzheimer's or schizophrenia). Job opportunities and social isolation could be at risk because of this information.

Ishai Y, 2018, The SMC protocols, despite the mathematical proofs that have been developed, are still not extensively utilised. This may be due to a lack of understanding of their capabilities, the complexity of their solutions, the need for coordination among the various sites, or the fact that they are not efficient in all situations. SMC protocols' inefficiency is one of their most glaring flaws. Inefficient SMC processes are a direct result of communication breakdowns. Most SMC research focuses on reducing the quantity of messages exchanged between the various parties and, as a result, reducing the performance difference between secure and non-secure protocol implementations.

In 2014, Dwork, C., published a paper titled, "Analysis of the Just like data types and integrity constraints for our database are defined during schema definition, so are the cryptographic safeguards provided by Jana administrators. The SQL aggregation operators, such as SUM and COUNT, can have differential privacy imposed on them if they want it. After query answers have been provided, this provides some level of data security. It is Jana's differential privacy protection algorithms that use secret sharing algorithms to compute and apply query results that are never "in the clear."

Mazloom, S. 2017, New methods of computing distributed noise that are compatible with SPDZ or other secret-shared computations have been sought out by Jana in order to protect query results while maintaining differential privacy. Additionally, Rebecca Wright and Anand Sarwate at Rutgers are currently improving their methods in order to further their research. Dov Gordon at George Mason University has developed a more efficient data access mechanism as a result of Jana's desire to improve secure computing performance.

3. RESEARCH PROBLEM AND METHODOLOGY

SMC ideal model is taken into consideration in this study because it always has a TTP that can be trusted by both parties. Computation and dissemination of results to all parties are tasks assigned to the TTP. Consequently, SMC solutions are designed to address these challenges without revealing the personal information of the people involved. It is possible to limit eventual privacy loss by adopting distributed randomization algorithms that preserve individual's personal data while still utilizing packetizing and pseudo-randomization.

3.1 MOTIVATION

Collaborative computation has been made possible by digitization since so many individuals are now connected to the internet, allowing them to undertake joint computations for mutual gain. This group of people could be mutually or somewhat trusted, or they could be rivals or adversaries. Problem solved if both parties trust each other, but difficult to undertake collaborative computation if just one party does. When working on sensitive information in groups, there is a general sense of trepidation among the participants.

As networking, cloud computing, and big data become more prevalent, there is an enormous difficulty in preserving picabytes of data generated each day from a wide range of sources while ensuring the privacy of the individuals involved. Privacy regulations apply to this data, thus it must be guarded against unauthorised access. There has been a conscious deficiency throughout this procedure that a few participants purposely provide incorrect data, resulting in an inaccurate result. To address these issues, the researcher came up with a series of models.

3.2 PROBLEM DEFINITION

Computational techniques for preserving privacy using secure multi-party computation protocols" is the research problem statement to meet the stated motivation. Assume there are "n" private parties, "m" anonymizers, and "DB" or "f(x1, x2... xn)" TTP with the database or computing function. There is no additional information given to other entities participating in computations when TTP performs a database query 'Q' traversing tables in the database and returns the result. Collaborative computation environments are depicted in Figure 3.1.

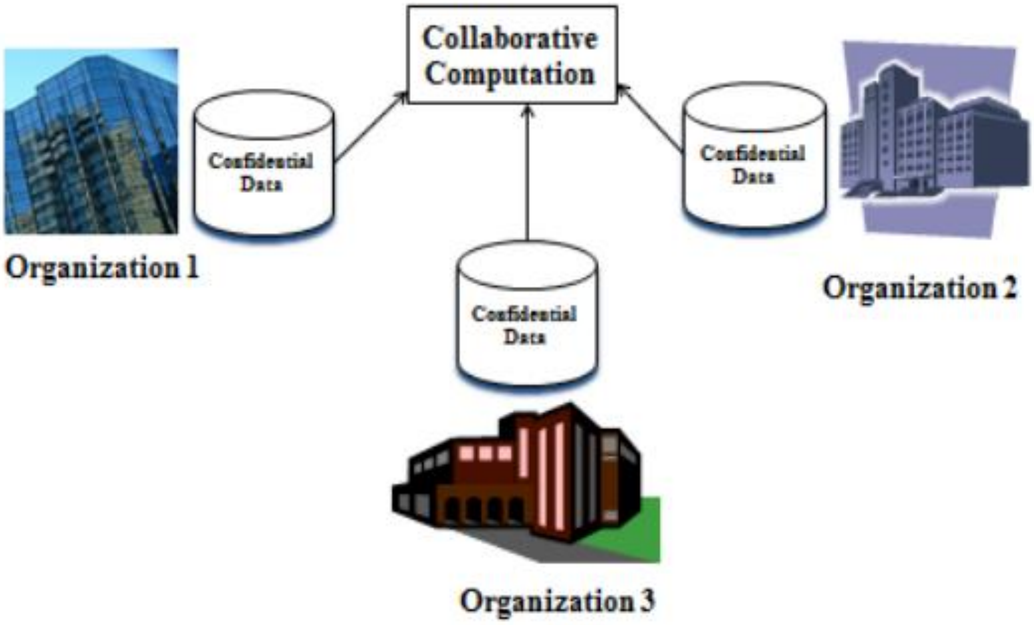


Figure 3.1: Computational Environment Model for Group Collaboration

3.3 OBJECTIVES OF RESEARCH

The objectives of this research work are executed in following manner:

Determine whether or not SMC is necessary or required.

- To create a multi-layered SMC architecture.
- Computational methods for protecting privacy are to be designed and developed.
- Anonymizers and TTP can't see the real data.
- Real-world testing of the above modules.
- To ensure that the module works properly before and after it is implemented.

3.4 RESEARCH METHODOLOGY

Figure 3.2 depicts the research methodology used.

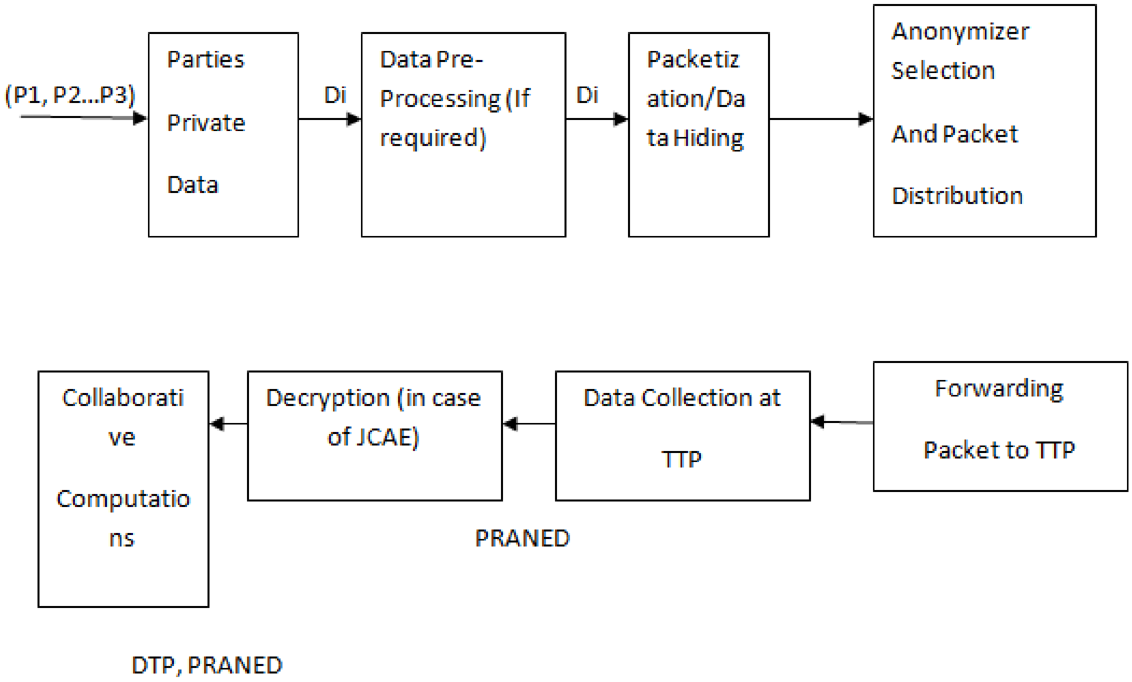

(P1, P2...P3)
Parties Private Data
Di
Data Pre-Processing (If required)
Di
Packetization/Data Hiding
Anonymizer Selection And Packet Distribution
Forwarding Packet to TTP
Data Collection at TTP
Decryption (in case of JCAE)
Collaborative Computations
PRANED
DTP, PRANED

Figure 3.2: Research Methodology

Research methodology and empirical methods are discussed in this section. There is an outline of the planned study's scope and limitations in this document. Analyzing current approaches like mismatched circuits, oblivious transfers, trusted hardware tokens, linear branching and neuronal networks, linear regression, and game theory is ongoing. To address the shortcomings of past methods, new research is carried out in order to develop better protocols. Anonymizers, party sizes, and other quantitative variables are all part of this study's design.

Input: Using a local network or the internet, one can provide input for collaborative computation as an individual party.

Pseudo-Randomization: In the proposed secure sum protocols, pseudo-random numbers are generated dynamically and inserted into plain data packets to protect an individual's sensitive information. A single pseudo-random number is used in the first protocol (JCRA), whereas many pseudo-random numbers are used in the second protocol (DRSS) in order to enhance data secrecy.

Encryption: One of the proposed protocols (JCAE) uses a packetization-based encryption approach to provide data confidentiality and security. An Asymmetric algorithm is used for experimentation.

Packetization: To ensure privacy, pseudorandomization and encryption are employed. The packetization process is used to safeguard communications from an attack. Despite the attacker receiving a packet from a particular party, the chances of getting all of that party's packets are extremely low due to packetization.

Develop a theoretical framework: Once the input type, pseudorandomization, encryption, and packetization techniques are selected, a layered architecture is used to build the theoretical basis for computation. Data can be sent from one layer to the next via a predefined function in each one of these layers. Following the validation of all packets received by the computing authority (TTP) at the topmost layer, the result of collaborative computations is broadcasted.

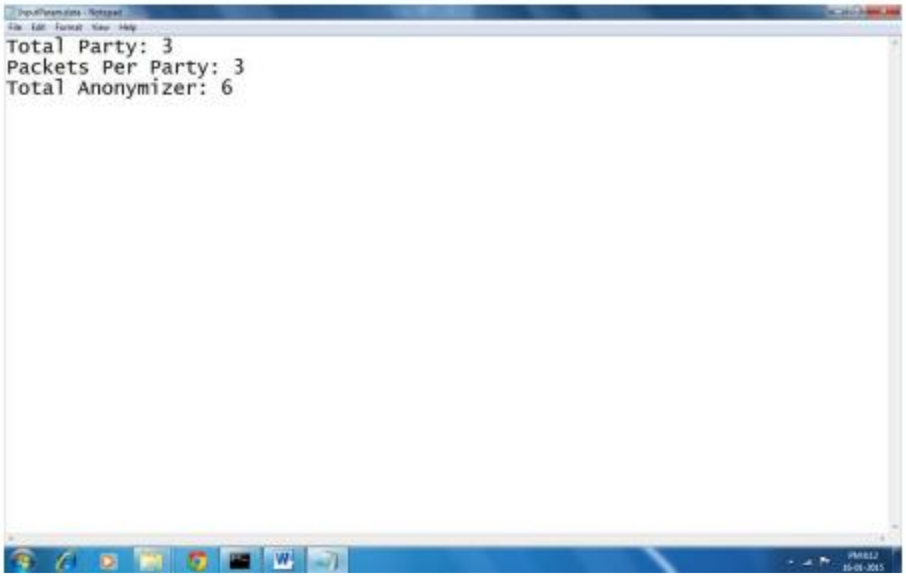
Data Sources: Data can be gathered in two ways. Use a randomization function to generate data locally or across a network of users. The results of previous studies were usefully analysed.

Performance Analysis: Data is gathered from all parties and then the algorithm is run based on the algorithm that was chosen. When evaluating the performance, various scenarios, such as a malicious party, an honest or semihonest party, and the turnaround time, are taken into account.

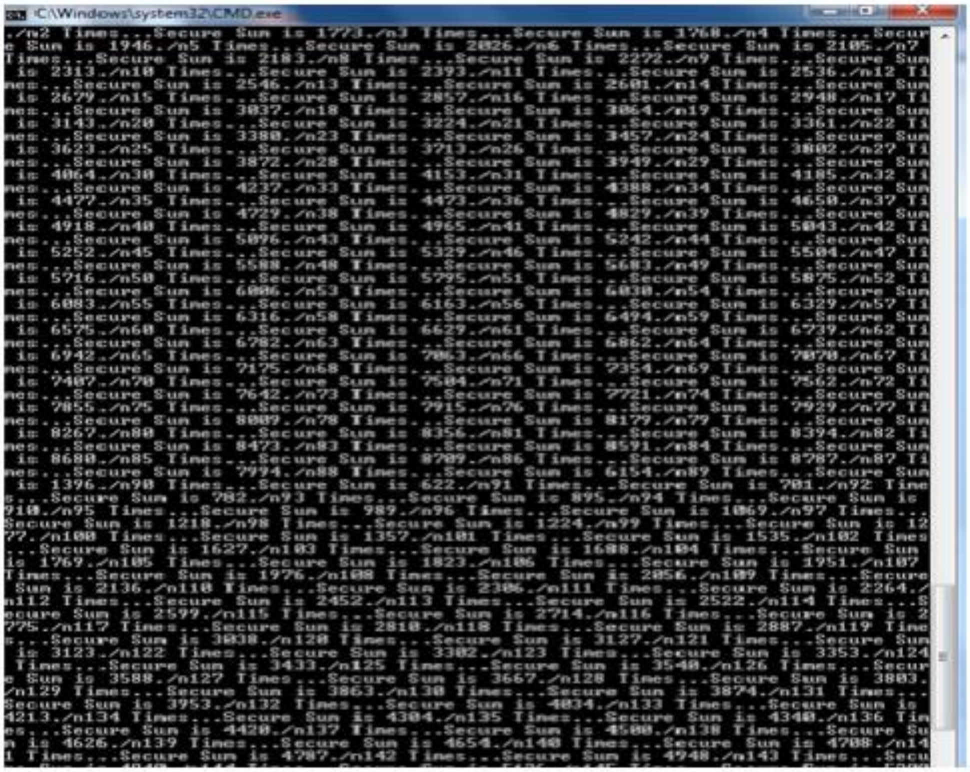
4. RESULTS AND ANALYSIS

The complexity of the protocols given is proportional to the number of persons involved in collaborative computations. C++ and a crypto C++ library are also used to simulate and analyse the protocol. As a client, we used a 1.66 GHz Intel core2 duo processor T5450 with 2 GB of RAM to compute the average run time. An input 32-bit positive integer is used to generate a pseudo-random number using the random function from [0-999] secure sum protocols called 'r'.

Web services are used to run the simulation in a networked environment. The parties involved in collaborative computations are the focus of our protocols' complexity. C# and the.NET library are used to simulate and analyse the protocol's performance. Intel Core i7 2.70GHz and 16GB RAM are used in this web server system. Microsoft's Internet Information Server (IIS) version 7.5 is used to host web services and WCF services. Firefox Mozilla 35.0 and Google Chrome 40.0 are the current web browsers. For the secure sum protocols JCRA and DRSS, the input data has a length of 32 bits, and r is generated using the Random class from the.NET library with a range of [0-999]. Asymmetric 128-bit keys are generated at registration time in JCAE using RSA (as well as the class from the.NET library, RSACrytpoServiceProvider)

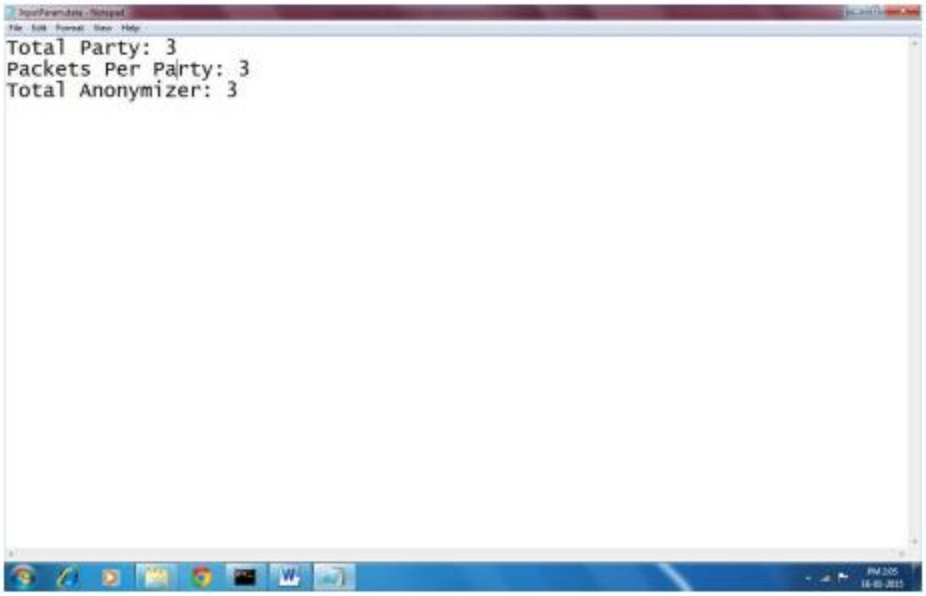


```
Total Party: 3
Packets Per Party: 3
Total Anonymizer: 6
```

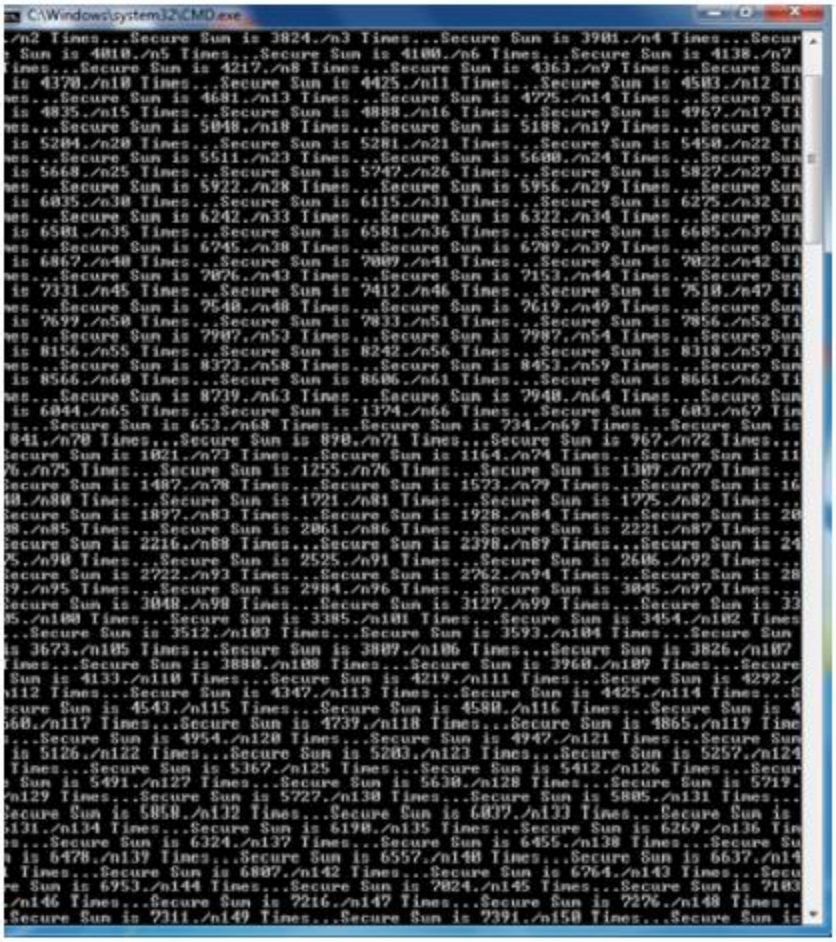


```
./n2 Times...Secure Sum is 1773./n3 Times...Secure Sum is 1768./n4 Times...Secur
e Sum is 1946./n5 Times...Secure Sum is 2026./n6 Times...Secure Sum is 2105./n7
Times...Secure Sum is 2183./n8 Times...Secure Sum is 2272./n9 Times...Secure Sum
 is 2313./n10 Times...Secure Sum is 2393./n11 Times...Secure Sum is 2536./n12 Ti
mes...Secure Sum is 2546./n13 Times...Secure Sum is 2601./n14 Times...Secure Sum
 is 2679./n15 Times...Secure Sum is 2857./n16 Times...Secure Sum is 2948./n17 Ti
mes...Secure Sum is 3037./n18 Times...Secure Sum is 3064./n19 Times...Secure Sum
 is 3143./n20 Times...Secure Sum is 3224./n21 Times...Secure Sum is 3361./n22 Ti
mes...Secure Sum is 3380./n23 Times...Secure Sum is 3457./n24 Times...Secure Sum
 is 3623./n25 Times...Secure Sum is 3713./n26 Times...Secure Sum is 3802./n27 Ti
mes...Secure Sum is 3872./n28 Times...Secure Sum is 3949./n29 Times...Secure Sum
 is 4064./n30 Times...Secure Sum is 4153./n31 Times...Secure Sum is 4185./n32 Ti
mes...Secure Sum is 4237./n33 Times...Secure Sum is 4388./n34 Times...Secure Sum
 is 4477./n35 Times...Secure Sum is 4473./n36 Times...Secure Sum is 4650./n37 Ti
mes...Secure Sum is 4729./n38 Times...Secure Sum is 4829./n39 Times...Secure Sum
 is 4918./n40 Times...Secure Sum is 4965./n41 Times...Secure Sum is 5043./n42 Ti
mes...Secure Sum is 5096./n43 Times...Secure Sum is 5242./n44 Times...Secure Sum
 is 5252./n45 Times...Secure Sum is 5329./n46 Times...Secure Sum is 5504./n47 Ti
mes...Secure Sum is 5588./n48 Times...Secure Sum is 5683./n49 Times...Secure Sum
 is 5716./n50 Times...Secure Sum is 5795./n51 Times...Secure Sum is 5875./n52 Ti
mes...Secure Sum is 6006./n53 Times...Secure Sum is 6030./n54 Times...Secure Sum
 is 6083./n55 Times...Secure Sum is 6163./n56 Times...Secure Sum is 6329./n57 Ti
mes...Secure Sum is 6316./n58 Times...Secure Sum is 6494./n59 Times...Secure Sum
 is 6575./n60 Times...Secure Sum is 6627./n61 Times...Secure Sum is 6739./n62 Ti
mes...Secure Sum is 6782./n63 Times...Secure Sum is 6862./n64 Times...Secure Sum
 is 6942./n65 Times...Secure Sum is 7063./n66 Times...Secure Sum is 7070./n67 Ti
mes...Secure Sum is 7175./n68 Times...Secure Sum is 7354./n69 Times...Secure Sum
 is 7407./n70 Times...Secure Sum is 7504./n71 Times...Secure Sum is 7562./n72 Ti
mes...Secure Sum is 7642./n73 Times...Secure Sum is 7721./n74 Times...Secure Sum
 is 7855./n75 Times...Secure Sum is 7915./n76 Times...Secure Sum is 7929./n77 Ti
mes...Secure Sum is 8009./n78 Times...Secure Sum is 8179./n79 Times...Secure Sum
 is 8267./n80 Times...Secure Sum is 8356./n81 Times...Secure Sum is 8394./n82 Ti
mes...Secure Sum is 8473./n83 Times...Secure Sum is 8591./n84 Times...Secure Sum
 is 8680./n85 Times...Secure Sum is 8709./n86 Times...Secure Sum is 8787./n87 Ti
mes...Secure Sum is 7994./n88 Times...Secure Sum is 6154./n89 Times...Secure Sum
 is 1396./n90 Times...Secure Sum is 622./n91 Times...Secure Sum is 701./n92 Time
s...Secure Sum is 782./n93 Times...Secure Sum is 895./n94 Times...Secure Sum is
910./n95 Times...Secure Sum is 989./n96 Times...Secure Sum is 1069./n97 Times...
Secure Sum is 1218./n98 Times...Secure Sum is 1224./n99 Times...Secure Sum is 12
77./n100 Times...Secure Sum is 1357./n101 Times...Secure Sum is 1535./n102 Times
...Secure Sum is 1627./n103 Times...Secure Sum is 1688./n104 Times...Secure Sum
is 1769./n105 Times...Secure Sum is 1823./n106 Times...Secure Sum is 1951./n107
Times...Secure Sum is 1976./n108 Times...Secure Sum is 2056./n109 Times...Secure
 Sum is 2136./n110 Times...Secure Sum is 2306./n111 Times...Secure Sum is 2264./
n112 Times...Secure Sum is 2452./n113 Times...Secure Sum is 2522./n114 Times...S
ecure Sum is 2599./n115 Times...Secure Sum is 2714./n116 Times...Secure Sum is 2
775./n117 Times...Secure Sum is 2810./n118 Times...Secure Sum is 2887./n119 Time
s...Secure Sum is 3038./n120 Times...Secure Sum is 3127./n121 Times...Secure Sum
 is 3123./n122 Times...Secure Sum is 3302./n123 Times...Secure Sum is 3353./n124
 Times...Secure Sum is 3433./n125 Times...Secure Sum is 3540./n126 Times...Secur
e Sum is 3588./n127 Times...Secure Sum is 3667./n128 Times...Secure Sum is 3803.
/n129 Times...Secure Sum is 3863./n130 Times...Secure Sum is 3874./n131 Times...
Secure Sum is 3953./n132 Times...Secure Sum is 4034./n133 Times...Secure Sum is
4213./n134 Times...Secure Sum is 4304./n135 Times...Secure Sum is 4340./n136 Tim
es...Secure Sum is 4420./n137 Times...Secure Sum is 4500./n138 Times...Secure Su
n is 4626./n139 Times...Secure Sum is 4654./n140 Times...Secure Sum is 4708./n14
1 Times...Secure Sum is 4787./n142 Times...Secure Sum is 4948./n143 Times...Secu
```

Figure 4.1: Screen shot of JCRA execution for increasing anonymizers.



```
Total Party: 3
Packets Per Party: 3
Total Anonymizer: 3
```



```
./n2 Times...Secure Sum is 3824./n3 Times...Secure Sum is 3901./n4 Times...Secur
e Sum is 4010./n5 Times...Secure Sum is 4100./n6 Times...Secure Sum is 4138./n7
Times...Secure Sum is 4217./n8 Times...Secure Sum is 4363./n9 Times...Secure Sum
 is 4370./n10 Times...Secure Sum is 4425./n11 Times...Secure Sum is 4503./n12 Ti
mes...Secure Sum is 4681./n13 Times...Secure Sum is 4775./n14 Times...Secure Sum
 is 4835./n15 Times...Secure Sum is 4888./n16 Times...Secure Sum is 4967./n17 Ti
mes...Secure Sum is 5048./n18 Times...Secure Sum is 5188./n19 Times...Secure Sum
 is 5204./n20 Times...Secure Sum is 5281./n21 Times...Secure Sum is 5450./n22 Ti
mes...Secure Sum is 5511./n23 Times...Secure Sum is 5600./n24 Times...Secure Sum
 is 5668./n25 Times...Secure Sum is 5747./n26 Times...Secure Sum is 5827./n27 Ti
mes...Secure Sum is 5922./n28 Times...Secure Sum is 5956./n29 Times...Secure Sum
 is 6035./n30 Times...Secure Sum is 6115./n31 Times...Secure Sum is 6275./n32 Ti
mes...Secure Sum is 6242./n33 Times...Secure Sum is 6322./n34 Times...Secure Sum
 is 6501./n35 Times...Secure Sum is 6581./n36 Times...Secure Sum is 6685./n37 Ti
mes...Secure Sum is 6745./n38 Times...Secure Sum is 6789./n39 Times...Secure Sum
 is 6867./n40 Times...Secure Sum is 7009./n41 Times...Secure Sum is 7022./n42 Ti
mes...Secure Sum is 7076./n43 Times...Secure Sum is 7153./n44 Times...Secure Sum
 is 7331./n45 Times...Secure Sum is 7412./n46 Times...Secure Sum is 7510./n47 Ti
mes...Secure Sum is 7540./n48 Times...Secure Sum is 7619./n49 Times...Secure Sum
 is 7699./n50 Times...Secure Sum is 7833./n51 Times...Secure Sum is 7856./n52 Ti
mes...Secure Sum is 7907./n53 Times...Secure Sum is 7987./n54 Times...Secure Sum
 is 8156./n55 Times...Secure Sum is 8242./n56 Times...Secure Sum is 8318./n57 Ti
mes...Secure Sum is 8373./n58 Times...Secure Sum is 8453./n59 Times...Secure Sum
 is 8566./n60 Times...Secure Sum is 8606./n61 Times...Secure Sum is 8661./n62 Ti
mes...Secure Sum is 8739./n63 Times...Secure Sum is 7940./n64 Times...Secure Sum
 is 6044./n65 Times...Secure Sum is 1374./n66 Times...Secure Sum is 603./n67 Tim
es...Secure Sum is 653./n68 Times...Secure Sum is 734./n69 Times...Secure Sum is
 841./n70 Times...Secure Sum is 890./n71 Times...Secure Sum is 967./n72 Times...
Secure Sum is 1021./n73 Times...Secure Sum is 1164./n74 Times...Secure Sum is 11
76./n75 Times...Secure Sum is 1255./n76 Times...Secure Sum is 1309./n77 Times...
Secure Sum is 1487./n78 Times...Secure Sum is 1573./n79 Times...Secure Sum is 16
40./n80 Times...Secure Sum is 1721./n81 Times...Secure Sum is 1775./n82 Times...
Secure Sum is 1897./n83 Times...Secure Sum is 1928./n84 Times...Secure Sum is 20
08./n85 Times...Secure Sum is 2061./n86 Times...Secure Sum is 2221./n87 Times...
Secure Sum is 2216./n88 Times...Secure Sum is 2398./n89 Times...Secure Sum is 24
75./n90 Times...Secure Sum is 2525./n91 Times...Secure Sum is 2606./n92 Times...
Secure Sum is 2722./n93 Times...Secure Sum is 2762./n94 Times...Secure Sum is 28
89./n95 Times...Secure Sum is 2984./n96 Times...Secure Sum is 3045./n97 Times...
Secure Sum is 3048./n98 Times...Secure Sum is 3127./n99 Times...Secure Sum is 33
05./n100 Times...Secure Sum is 3385./n101 Times...Secure Sum is 3454./n102 Times
...Secure Sum is 3512./n103 Times...Secure Sum is 3593./n104 Times...Secure Sum
is 3673./n105 Times...Secure Sum is 3809./n106 Times...Secure Sum is 3826./n107
Times...Secure Sum is 3880./n108 Times...Secure Sum is 3960./n109 Times...Secure
 Sum is 4133./n110 Times...Secure Sum is 4219./n111 Times...Secure Sum is 4292./
n112 Times...Secure Sum is 4347./n113 Times...Secure Sum is 4425./n114 Times...S
ecure Sum is 4543./n115 Times...Secure Sum is 4580./n116 Times...Secure Sum is 4
660./n117 Times...Secure Sum is 4739./n118 Times...Secure Sum is 4865./n119 Time
s...Secure Sum is 4954./n120 Times...Secure Sum is 4947./n121 Times...Secure Sum
 is 5126./n122 Times...Secure Sum is 5203./n123 Times...Secure Sum is 5257./n124
 Times...Secure Sum is 5367./n125 Times...Secure Sum is 5412./n126 Times...Secur
e Sum is 5491./n127 Times...Secure Sum is 5630./n128 Times...Secure Sum is 5719.
/n129 Times...Secure Sum is 5727./n130 Times...Secure Sum is 5805./n131 Times...
Secure Sum is 5850./n132 Times...Secure Sum is 6037./n133 Times...Secure Sum is
6131./n134 Times...Secure Sum is 6190./n135 Times...Secure Sum is 6269./n136 Tim
es...Secure Sum is 6324./n137 Times...Secure Sum is 6455./n138 Times...Secure Su
m is 6478./n139 Times...Secure Sum is 6557./n140 Times...Secure Sum is 6637./n14
1 Times...Secure Sum is 6807./n142 Times...Secure Sum is 6764./n143 Times...Secu
re Sum is 6953./n144 Times...Secure Sum is 7024./n145 Times...Secure Sum is 7103
./n146 Times...Secure Sum is 7216./n147 Times...Secure Sum is 7276./n148 Times..
.Secure Sum is 7311./n149 Times...Secure Sum is 7391./n150 Times...Secure Sum is
```

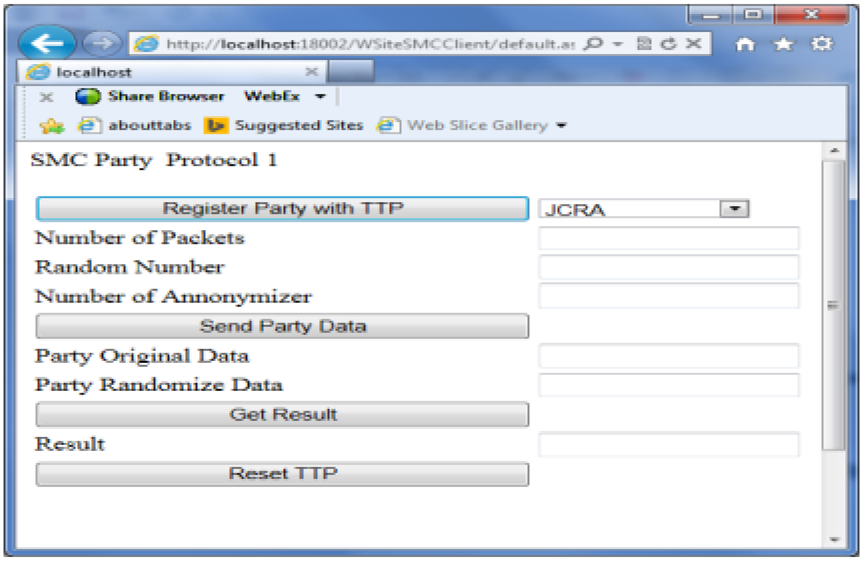
Figure 4.2: Screen shot of JCRA execution for same number of parties, packets and anonymizers

Fig. 4.1 and 4.2 show a screen shot of the procedure JCRA being executed. Using ASP.NET web services and WCF, web models of the protocols JCRA, DRSS, and JCAE were built to test the research hypothesis (Windows Communication Foundation).

WebMethod

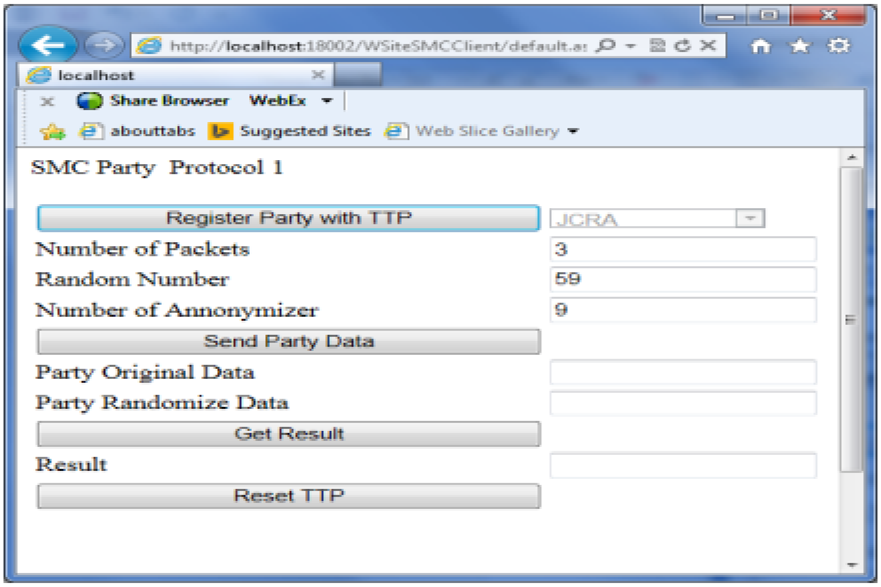
```
public int [] PreparePartyDataRandomly(string strPartyName, int[] nPartyData, int nPacket, int nRandNum)

 {

// based on the nPartyData, add the randon number passed and divide into packet and then return string array of numbers seperated by comma

int len = nPartyData.Length;

int nRandBit = nRandNum / len;

int nRandLeftOver = nRandNum % len;

List li = new List();

foreach (int nData in nPartyData)

{

if (li.Count == 0)

li.Add(nData + nRandBit + nRandLeftOver);

else

li.Add(nData + nRandBit );

}

int [] nRandomizePartyData = li.ToArray();

return nRandomizePartyData;
```

}



SMC Party Protocol 1

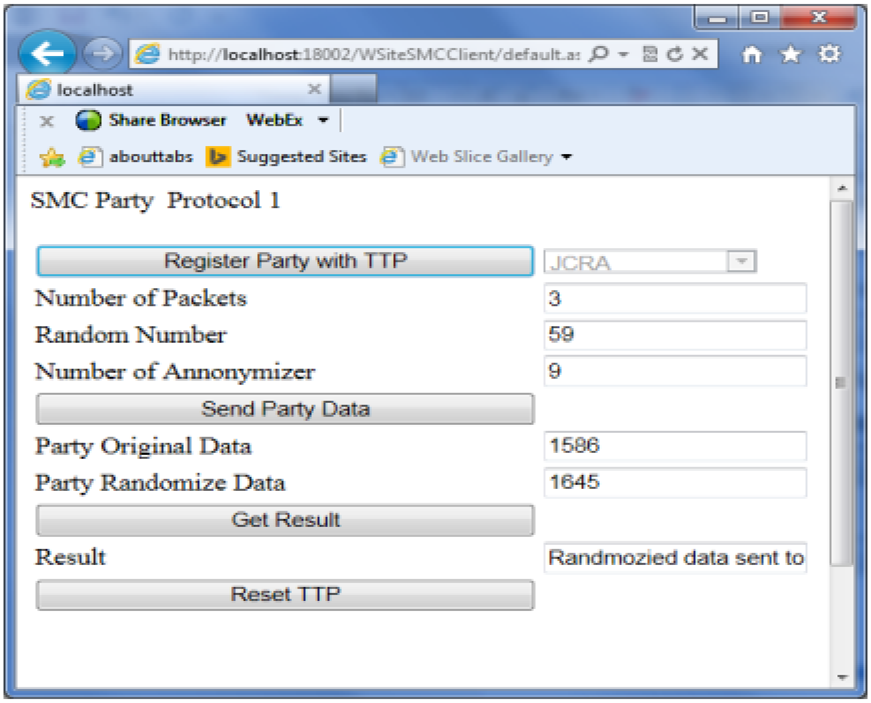
Register Party with TTP	JCRA
Number of Packets	
Random Number	
Number of Annonymizer	
Party Original Data	
Party Randomize Data	
Result	



SMC Party Protocol 1

Register Party with TTP	JCRA
Number of Packets	3
Random Number	59
Number of Annonymizer	9
Party Original Data	
Party Randomize Data	
Result	

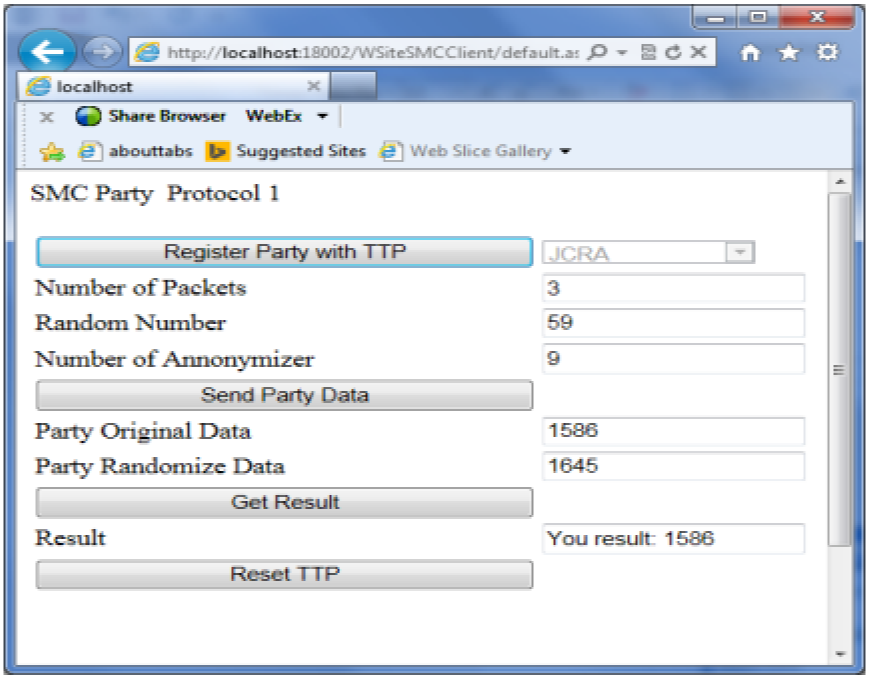
Figure 4.3: Screen Shot of registration with TTP, protocol parameters are generated.



SMC Party Protocol 1

JCRA

Number of Packets	3
Random Number	59
Number of Annonymizer	9
Party Original Data	1586
Party Randomize Data	1645
Result	Randmozied data sent to



SMC Party Protocol 1

JCRA

Number of Packets	3
Random Number	59
Number of Annonymizer	9
Party Original Data	1586
Party Randomize Data	1645
Result	You result: 1586

Figure 4.4: Screen shot of get the computation result.

CONCLUSION

Confidential access to data collected, used, stored, or otherwise protected as confidential is referred to as a "confidentiality leak." Confidentiality losses can be both personal and financial, depending on the nature of the breach. The asymmetric encryption techniques methodology used in this study opened up new avenues of research in multi-party computation. In the future, this work could be expanded to include more complex functionality in a variety of simulation setups. Techniques for protecting privacy during secure multi-party computations were designed and developed as part of this research. In the first place, a secure sum protocol called JCRA was designed, and the parameters that affect the security and confidentiality of individual participants were presented. Then, the protocol was evaluated for computation complexity, confidentiality, and security for some problem.

REFERENCES

1. P.Yoganandhini, “Privacy Preserving Data Mining Using Secure Multiparty Computation Based On Apriori and FpTree Structure of Fp-Growth Algorithm”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-3, January 2020.
2. The development of large-scale de-identified biomedical databases in the age of genomics-principles and challenges. Dankar FK, Ptitsyn A, Dankar SK Hum Genomics. 2018 Apr 10; 12(1):19.
3. Ishai Y, Mittal M, Ostrovsky R. On the Message Complexity of Secure Multiparty Computation. 21st IACR International Workshop on Public Key Cryptography; 2018; Rio de Janeiro, Brazil. 2018. Mar 25, pp. 698–711. [Google Scholar] [Ref list]
4. Dwork, C., Roth, A. et al (2014) The algorithmic foundations of differential privacy. Foundations Trends Theor. Comput. Sci., 9, 211–407.
5. Mazloom, S. and Gordon, S.D. (2017). Differentially private access patterns in secure computation. Cryptology ePrint Archive, Report 2017/1016. https://eprint.iacr.org/2017/1016.
6. 50. Qingkai M, Wei H, I-Ling Y, and Bastani F, “Multiparty computation with full computational power and reduced overhead”, proceeding of eighth IEEE international symposium on high assurance system engineering, 241-248, 25-26 March, 2004.
7. Rabin M, “How to exchange secrets by oblivious transfer”, Tech. Report Memo TR-81, Aiken Computation Laboratory, 1981.
8. Ronald C, Ivan D, “Multi-party computation: an introduction”, Lecture Notes, 2004.
9. Raymond W, Jiuyong L, WaiChee A and Wang K, "(α, k)-anonymity: an enhanced k-anonymity model for privacy preserving data publishing", proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining, 2006.
10. Rane S, Wang Y, Draper S, and Ishwar P, "Secure Biometrics: Concepts, Authentication Architectures and Challenges", arXiv preprint arXiv:1305.4832, 2013.
11. Srivatsava R, Kasiviswanathan S P, and Smith A, "Composition attacks and auxiliary information in data privacy", proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining, 2008.
12. Sheikh R, Kumar B, and Mishra D K, “Privacy-Preserving k-Secure Sum Protocol”, International Journal of Computer Science and Information Security, 6(2), 184-188, November, 2009.
13. Sheikh R, Kumar B, and Mishra D K, "Changing Neighbors k Secure Sum Protocol for Secure Multi Party Computation", arXiv preprint arXiv:1002.2409, 2010.
14. Sadeghi A, Schneider T, and Winandy M, "Token-based cloud computing." Trust and Trustworthy Computing. Springer Berlin Heidelberg, 417-429, 2010.
15. Sheikh R, Kumar B, and Mishra D K, “A distributed k-secure sum protocol for secure multi-party computations", arXiv preprint arXiv:1003.4071, 2010.
16. Sheikh R, Kumar B, and Mishra D K, "A Modified ck-Secure Sum Protocol for Multi-Party Computation", arXiv preprint arXiv:1002.4000, 2010.
17. Sheikh R, Kumar B, and Mishra D K, "Secure Multiparty Computation: From Millionaires Problem to Anonymizer", Information Security Journal A Global Perspective, 2011.
18. Trevathan J, “Security anonymity and trust in electronic auctions,” Crossroad archive, ACM Press, 11(3), May, 2005.
19. Teo S G, Vincent L, and Shuguo H, "A Study of Efficiency and Accuracy of Secure Multiparty Protocol in Privacy-Preserving Data Mining", Advanced Information Networking and Applications Workshops (WAINA), IEEE 26th International Conference, 85-90, 2012.
20. Verykios V S, Elmagarmid A K, Elisa B, Saygin Y, and Elena D, “Association rule hiding”, in IEEE transactions on knowledge and data engineering, 15(3), May/June, 2003.