DECENTRALIZED AND CYBER-SECURITY BASED INFORMATION SHARING COMMUNICATION SUITE

Aloush Abdul Rahman Shamrokh Al-Otaibi
Masters student, Faculty of Computing and Information Technology, University of Bisha, Bisha, Saudi Arabia

The recent advancements in the field of cybersecurity demanded efficient information sharing and also that has been acknowledged for many years as a prominent factor to the cybersecurity community. At present, there is no standard infra for Information sharing and mostly utilizes non-standard data structural sources. To build up a secure infra for information sharing against possible vicious threats, a perfect cyber defense system is found to be the need of the hour. Cybersecurity investigators and architects head to uphold the integrity, availability, and confidentiality of selective information and data management systems via several cyber defense systems that defend any network and its systems from cyberpunks.With the enlargement in communicating networks, vulnerability to cyberpunks also raises. So, besides the concepts of cybersecurity, any key players need to build up a decentralized network system which enhances the robustness and renders an efficient resolution against cyberpunks and threat in the large-scale organization process. Even if attacker's minds blockingthe entire network system,decentralization conception prevents such infiltration to access entire data. Thus, a decentralized cyber defense system has become an outstanding infra for any organization. However, establishing such kind of defense system is challenged mainly to the adaptation to a new decentralized network for privacy based information sharing among different blocks of the organization at a different location. Hence, we propose a secured information schema that enables the secured communication in encrypted format among different data points/data centers of the organization. Moreover, the resultants of the proposed concept showbetter complexity in terms of communication and computation costs. This conception delineated in this article once accomplished at a large-scale would render the basic building blocks for springing up an extremely efficacious cybersecurity information sharing system in the decentralized network.

Keywords:Cybersecurity, Decentralization,Homomorphic Encryption, ElGamal cryptosystem.

1. INTRODUCTION

Most of the modern and complex networks progressively demand highly specialized conceptual cybersecurity knowledge. Moreover, the requirement and welfares of information sharing for resistant and firm cybersecurity are unambiguously recognized by all stakeholders, including commercial-grade and non-commercial-grade organizations, and private and governmental agencies.Organizations are aggregating an enormous amount of cybersecurity data internally and externally for employing better protection against threats and to defend a firm cybersecurity posture.Most of the researchers have spent substantialattempts to deal with the effects of cybersecurityinformation sharing and proposed many ideas to counter those sharing issues and also, to balanceboth the benefits and costs of applying quantitativeand qualitative methods.

1.1 Scope of Collaborative Security in Decentralized Network

From [1], thecollaborative security has been delineated as “ratherthan utilizing centrally supervised policies, the data points or centers in the organization may share andcollect cybersecurity associated knowledge to attain the security concerned decisions”. The objective of this collaborationism is to attain the decisions more efficaciously as the enormous data are available, the precise decisioncan be attainedon utilizing that selective information. So the“collaborativesecurity” plays a key role among various security systemsby portioning out various security-related information to make moresensible and effective decisiveness. This collaborative securitysystem has been employed in manysecurity-related domainssuch as intrusion detection, anti-malware, anti-spam, etc. Hence the collaborative security manages to behave in adecentralized manner to bring down the dependency on a single or centralized server and in-return deliverfirm data control to the different data-points/centersinvolved in the communications of the organization. It explores the importance of decentralization in providing security to any system.

1.2. The Necessity of Decentralized Cybersecurity

Issues such as eminentspatiality of the node/system, incertitude,geographical detachment of components, delays in the communicating network, and rapid attacks by cyberpunks with the

motive of collapsing the entire network are factors that alarm the situation for the change from centralized decision making to decentralized control.A decentralized network is an environment that provides complete robustness by ensuring no single point of failure. The nodes/systemsinterconnected in the network are not dependent upon a single centralized device and hereby each node/system might be replicated with the network configurations.To avoid failure of the entire network system by external cyber-attacks, all the data-points/nodes in the network transmit selected information to all other known data-points/nodes, whether those adjacent data-points register the applicable data or not.

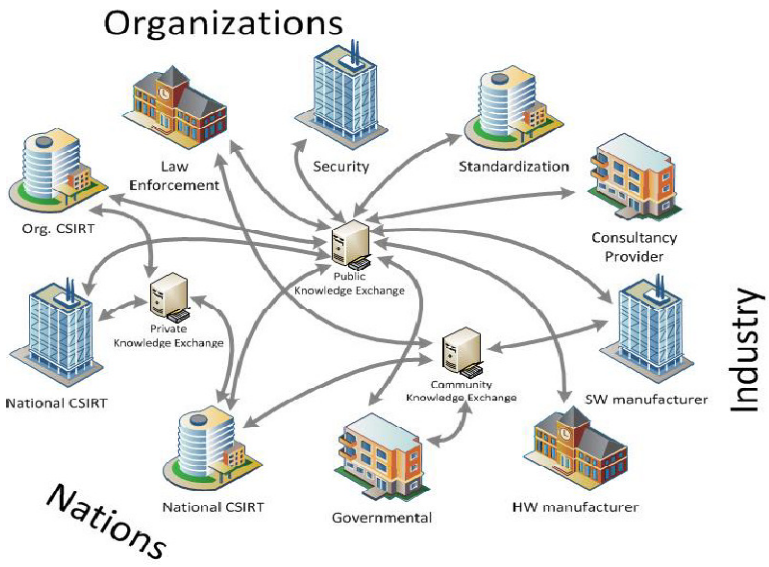

Figure 1: Concept of Knowledge sharing in Decentralized Network [47]

Normally, this information sharing approach uses BFS (Breadth-First Search) strategy which is referredto as the “message flooding approach”. To avoid infinite recursive data transmissions, to control the number of secured keys per information generationon a single request, every communicativeinformation is allotted with a special value calledthe “Time-To-Live (TTL)” value. Every data-pointshares this TTL info whichdecreases their value by 1 and only thatinfois forwarded, having positive TTL values. The merit of decentralized networks is that it does not demandnetwork structural maintenances proactively. In the decentralized network system, the members of a multicast in-group are segmented into lotsof smaller sub-groups that are regulated by different kind of sub-group controllers. This type of accessputs an end to the single point vulnerability issue as well as the “one-affect-N”problem and importantlyminimizes the re-keying computation cost.

1.3. Concern on Cybersecurity Attacks

The hypotheses of attacks are tremendous in decentralized networks. Most common attacks, as well as few suitable defense mechanisms that are adopted in the decentralized network system, are listed and discussed as,

i. Rational Attacks

For decentralized network services to be in effect, activeinterconnected data-point must collaborate, but a node/data-pointconstitutes a self-interestedposse, and cooperation cannot be expected or enforced all the time. A sensiblepresumption is that a large section of data-pointsare rational and will merely seek to reduce their consumption of the network's available resources while reducing the utilization of their own. To illustrate with an example, here some set of nodes might recognize that refusal of sharing of the required information, they save precious uploadable bandwidth. Specifically, in the instance of copyrighted substantial, information sharing can have the worst consequences. Hence it is illegal and quite easy for attackers to determine who is sharing specific information that may lead to heavy disaster. These are adequately good for the circumstances to promptdata-points in getting "self-interested". If a large set of data-points/nodes are becoming self-interested and decline to contribute, the entire network system may destabilize. Successful decentralized systems must be planned/designed to be robust against this ration attack and its mere consequences.

ii. File Poisoning

File poisoning attacks tend to be maneuver on the data plane and have turn exceedingly common in decentralized networks. This attack aims to interchange an informative file with a false one in the network that leads to inaccuracy especially during decision-making. This uninformative file is naturally of no use.To attack through this file poisoning, malicious data-points will incorrectly claim owning the desired file, and upon a postulation will respond with a polluted file.All these facts may enable the poisoned file with high availability throughout the network, and attract others to download it as the true one.Thus, the attackers have a variety of chances to breach the network system after such data pollution.

iii. Sybil Attack

Sybil attacks are constituent of the control plane class. The core idea behind this Sybil attack is to gain control over part of the network by enacting any single malicious identity as multiple identities. Once this representation has been accomplished, the attacker can breach and collapse the network activity through all possible events. For instance,the cyberpunks might attainsole responsibility for certain rightful files and prefer to spoil them with uninformative guidance. If the cyberpunks canlay his/herindistinguishability is a strategically unique way, the impairment and consequence will be high.

iv. Eclipse Attack

In the case of an eclipse attack, the cyberpunks try to gain control over a certain part of the network system through strategic routing paths.On the accomplishment of this early operation, the network system is separated into different sub-networks. Thus, for further communication, all data-point is made dependent on other sub-networks data-points. Besides this, all the informationmight have future possibilities to be routed through any one of the data-point controlled by cyberpunks. Here, each data-points are thus “eclipsed” to data-points that belong to other sub-network (likehigh-scale man-in-the-middle attacks). Sometimes, an eclipse attack could be the continuance of a Sybil attack. In sucha case, the cyberpunks will try to position their deceiver data-points on the strategic communication paths. Now the attacker can completely take over the control of each sub-network. If an attacker plans for an eclipse kind of attackcan attack the network throughthe following efficient ways.

- The attacker can attack the control plane are attacked inefficiently by rerouting all insecure messages.
- The attacker can make up one's data-point to drop all receivable unsecured messages, thus completely isolating the two sub-networks.

Finally, the communicable files to the genuine data-points are attacked by injecting misinformation or requesting the misguided fileon behalf of the genuine one. Thus these files are copied or cached along the path and slow down or halt the process of the entire network by rerouting all queries in a misguided way.

2. RELATED WORK

2.1. Collaborative security and Associative Methods

Most of the existing research work exhibits remarkable efforts to dig into the epitome of collaborative security and critical review affiliated methods. Nevertheless, the scopes of those efforts are frequentlylimited to particular areas, which is insufficient for systematic classification and analysis. The collaborativeattacks concerning the cybersecurityinformation sharing and the rudimentary secrecy challengeshave been examined in [2]–[6]. A theoretical account for privacypreservation of cybersecurity data sharing has beennominated by [4]. This strategyemploysa group signature to blot outthe identicalness of the organizations. Nevertheless, this strategy doesnot defend the key collaborator's information. Some delineation from [6] has prototyped thesecrecy issue in cybersecurity information sharing as a rulebetween attackers and organizations. Thoughthisframeworkaids the organizations to determine their apportioning strategy, it doesnot furnish any practical resolution to defend the fundamentalinformation. The article from [1] demonstratedaggregation of collaborativesecurity concerning research. The primaryconsequence is that they lackinsightful and detailed analysis with a precise summary. Thetheoretical aspects of[7]exhibited common units of a cooperative intrusiondetection system which most specifically admits the system security and informationsharing. They also delivered theprivacy preservation scheme onapportioning any highly protectivebasedinformation. The issues in collaborative intrusiondetection systems were depicted in [8]. They reviewedseveralorganized attacks that conventional intrusion detection systemscannotbe discovered. The article [8]presented a new sort of intrusiondetection system through a conjunctive lens. Apart fromthe aboveresearch exploits, theformer research investigated specificfacets of collaborative security measures, however, they did notconsider the integrality of the issue. The article in [9] reviewed multipleclasses of incorporated anomalies and deliversfundamental challengesfor each class. They also looked into a series of methodologiesto dealwith these incorporated anomalies as well as rigorouscomparability between those defined methods. The article in [10], with anillustration,discoursed one specificarea in collaborative intrusion detectionsystems thatwarn or alert correlation. Their research revieweda significant number of employed approaches towarn or alert correlationand demonstrated the weaknesses and strengths respectively.The author in [11] also carried a reviewof spam filteringapproaches,

especially those addressing with collaboration, andfurnishedsuccinct statements of the pragmatic applications.

2.2. Cybersecurity Infrastructure and its Sharing Communities

As the intensity of selective information available has sprung up exponentially,so has the research concern in collaborative data sharing. It isgenericallydistinguished across the several research project-based communitythat effective infrastructures are expected to alleviate such sharing.It is common in most Computer Security IncidentResponse Teams (CSIRTs) not to be an exception for employing effective cybersecurity, especially for data sharing. However, the majority of the functionchannelizedat the exploitation of comprehensive structures of the organization for datasharing which has been guided by other communities.To illustrate, biologyhas been a highlycontributive area in collaborative data sharing, sincenew DNA sequencingproficiencies have directed to the demand to managethe outcomes witha steeprise in the production of an amount of information.

Similarly, healthcare-associated data sharing has been avitaldomain of focus for any researchers concerning data sharing over the lastdecade. This segmentcovers-up some of the significant work exhibited inthose communities, spotlighting both fundamental research and complete systems.Concerning systems, SciPort [12] offers a centralized server-based,lightweight data integrating architecture, which incorporates andshares a schematic plan across different organizations, providing distributedevolution, schematic plan management, and sharing. ORCHESTRA from [13]is a tool employed to alleviatethe data sharing process when there is an improper consensus regarding how the vita; the info should be constituted,what isprecise, and which original references are authoritative. The context in reference [14]delineates a middleware model that endorses the aggregation of data and securesharing from heterogeneous information sources,meanwhile [15] nominates a privacy-preserving model tocolligatelarge-scale, loosely coupled data sources through a brokeringoverlay. Hyperion from [16] is a prototype modeled system that affirms datasharing particularly for a network of independent Peer Relational DatabaseManagement Systems (PDBMS) and [17] delineates a disseminateddata sharing system that admitsinformation sharing without sharedoutlines.

The majority of effort has been dedicated to other significantdomainsfor data sharing such as maintaining privacy while sharing secrete information[18]- [19],

incorporatingheterogeneous data sets [20], delineatingdata sharing policies [21], coaction [22], directionto uncertain data [23]-[24] and information evolution [25].Various tools that ensure data sharing solelypoint-out the cybersecurity community and few of them enforce solutions tosome of the fundamental problems keyed out in this paper. To illustrate, the Collective Intelligence Framework (CIF) [26] provides theindependent intake of data feeds regardless of the data models.

Likewise, the Model-based Analysis of Threat IntelligenceSources (MANTIS) [27] nominates a conciliatory data model to ensure thetolerance for diverse revisions and formats. Boththese toolsaidin finding advanced solutions in the way that the researchernominates. Othershave a more circumscribed and boundedset about to data models, but integratefeatures such as confederacy of various communities, for example,the Malware Information Sharing Platform (MISP) [28], whichhas benefitted grip in different communities (e.g. EU, NATO) andadmitsefficient sharing formats of malware data.

The Avalanche[29] systems and Collaborative Research into Threats (CRITs) [30]carry out the widely consented standards TAXII,MAEC, STIX, and CybOX, which can affirm largecommunities.Despite the ample amount of research work and the numerous prototype systems that have been evolved, no system has yetdeveloped into a widely recognizedfine yielding system. Although most of these systems are beneficial atfiguring out some issues (e.g., selective, sharing, privacy, heterogeneity), yet it is normally determinedthat none of the systems efficiently deal with all of theissues.

2.3. Types of Information to Be Shared

It’s been a high-end research question, “What type of information/data is trusted to be shared?” According to theCybersecurity Information Sharing Act (CISA) [31], the information that to be shared isdesignated into two types. They are

- Cyber-Threat Indicators and
- Defensive Measures.

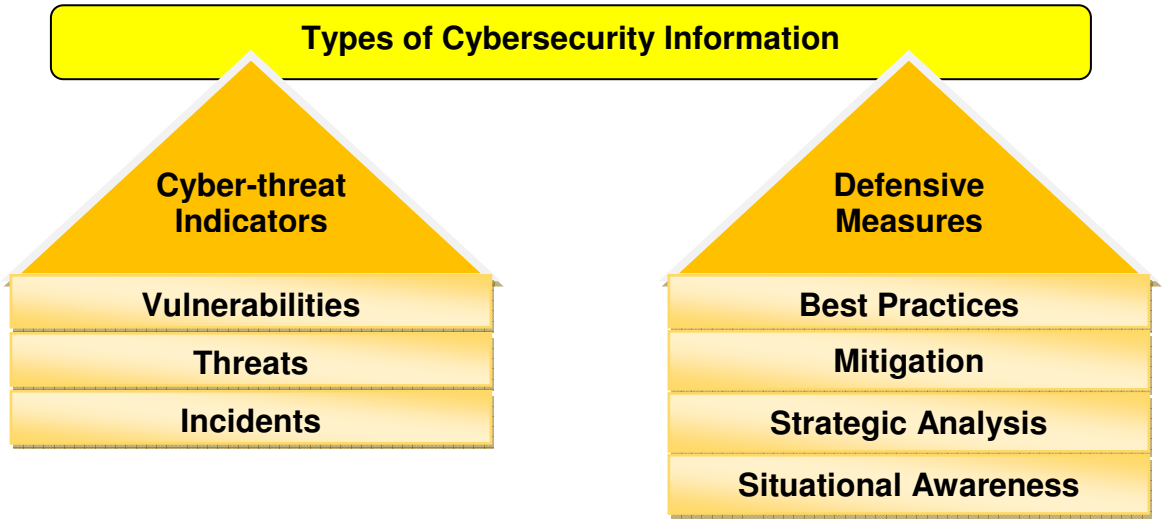

Figure. 2.1 Types of Cybersecurity Information (to be shared)

The differentiation between these twomajor types of information categories is either they possess higher risk or lower risk to both market value andprivacy of the sharing organization.Figure 2.1, depicts the combination of this classification based on [32].The cyber-threat indicators category constitutes vulnerabilities (impuissance that can beexploited), threats (possible severe issues), and incidents (particulars of cyber-attack events).All these kinds of information may cause a revelation of vitalcritical know-how of the organization that can damage itsreputation and as a consequence contract market value. Meanwhile, defensive measurescomprise best practices (data on most beneficial actionsagainst attacks), mitigation (forethoughts/precaution for future attacks), strategic analysis (employing informationto evolve effectual defensive measures), andsituational awareness (information to dealwith anincident).This kind of information generally does not havea greater risk to the organization.

2.4. Review on Existing Cybersecurity Solutions

In the field of cybersecurity, various solutionsare proposed through different states of art technologies such as

- Intrusion Detection System (IDS),
- Vulnerability Scanners,
- Network and Application Firewall, and
- Intrusion Prevention System (IPS).

i. Intrusion Detection System

Intrusion detection systems (IDS) are the kind of software projected to find the illegal approach/attack to the resources or system.Signatures based Intrusion Detection Systems (SIDS) key out “signatures” of experienced approaches/attacks and employ suitable form (pattern) matching algorithms [33] for attack detection and analysis [34].An anomaly-based system examines the remarkable feeding stream against constituted profile and sorts out all abnormal conduct as malicious [35]. Data Mining Methodologies for anomalydetection furnish the model for web application attacks/approaches based on the facts of statistical techniques [36].Ontology oriented IDS resolutions are utilized in information security. Raskin et al. [37] evolved the typical ontology for selective information integrity of any web recourses and encourage the usage of ontologyfor information security purposes. Landwehr et al. [34] exhibit aunique classification hierarchy of intrusion based on location, genesis, and means. Ning et al. [38] viewed a hierarchical model for the stipulation of different approaches/attacks and thoroughly patterned and examined the attributes and characteristics of attack.McHugh [39] concentrated on the classification of attacks/approaches concerned tothe protocol layer and Guha [40] stressed upon the examination of TCP/IP protocol stack along with its full constituted layers to assist as thebasis for attack taxonomy. Denker et al [41] aim thecontrol admittance through ontology evolved in DAML+OIL[42] but these organizations may not be fully utilizable due tomere representation of attack properties thus they areineffective for intrusion detection. Many research from have focused on the ontology defined an intrusion detection technique especially for networklayer attacks and also proposed the new approach to devolving an intrusion detection application. Ontology of Information Security delineatedthe formal vulnerabilities, threats, countermeasures, models assets, and their relations. Researchers in [43] concentrate on the usage of security ontology that can affirm the ISO/IEC 27001 certification and sustentation of security policies/guidelines.

ii. Vulnerability Scanners

Commonly, web application-oriented scanners are the automated tools that commence by crawling into files concerning web applications and then examine its web pages to detect the vulnerabilities in the developed application on utilizing the passive technique. Through this technique, the scanners render a thorough investigation into inputs and then examine the response against those inputs for anysecurity vulnerabilities [44].

iii. Network and Application Firewall

Most of the accounted cyber crimes are listed asexploiters of the applicationlayer. This became possible on the utilization of port 80 or 443(SSL), especially for business communication. Thus, these security solvents do not provide a perfect resolution to the application level threats. Although, it's been found that network firewalls are suitable only for securingthe internal network infra and communication activities of the organizations, still vulnerable to several application illicit approaches/attacks by the cyber crooks. The relevant and necessary solutions are shortlyexplicated along with limitations.

iv. Intrusion Prevention System

Intrusion Prevention systems are the software designed not only to detect the rise of vulnerabilities and unauthorized access to the resources butalso to prevent the secured information from unauthorized access.

3. SECURED INFORMATION SCHEMA

The primary contributions of the research work can be summarized as follows.

- A highly secured cybersecurity information sharing schema has been proposed for a decentralized network system in which secure communication is enabled especially for multi-domain organizations possessing different data-point.
- To avoid information threats during communication, a well-known encryption technique has been utilized. This encryption technique not only serves to secure confidential data but also prevents communicative data from malicious threats or possible vulnerabilities.
- A specialized Homomorphic Encryption protocol called "ElGamal cryptosystem" is employed for the better optimization of key generation, encryption, and decryption process.

3.1. Homomorphic Encryption

The proposed schema utilizesthe ElGamal cryptosystem [39] to leverage their homomorphic properties especially to perform the computations. The ElGamal encryption strategyis a probabilistic public-key encryption technique thatis compiled of encryption, key generation, and decryption process. Figure 3.1 depicts the basic homomorphic procedures.

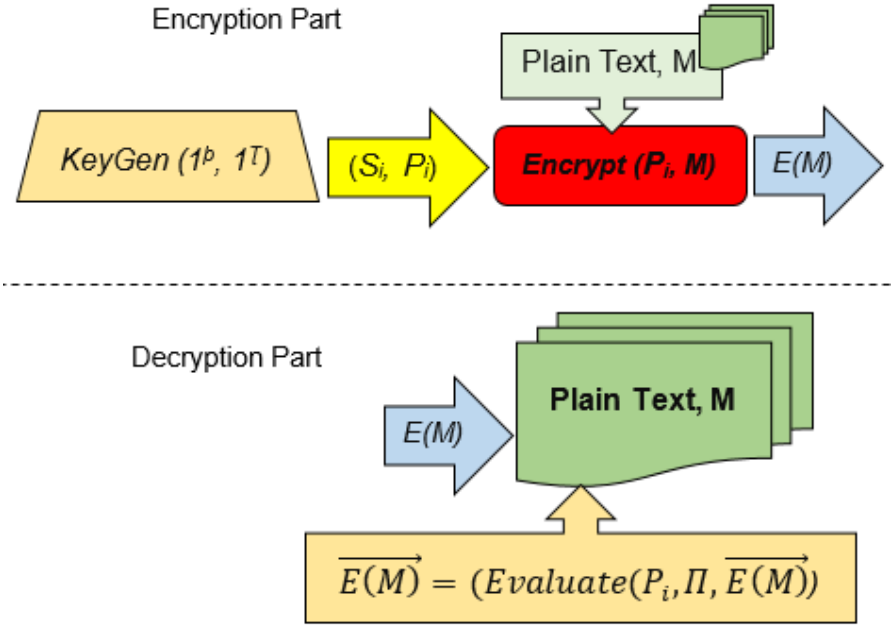

Figure 3.1. Homomorphic Procedure

To adapt to the decentralized network system, the distributed edition/version [45] of the ElGamal cryptosystem is employed. This cryptosystem highly supports both homomorphic multiplications as well as addition. Based upon several reviews, it was also found that the performance and computational efficiencies have been very effective in someof the recent researches done on privacy-preserving applications along with other standard cases of homomorphic encryption oriented applications.

The working mechanism of the ElGamal cryptosystem according to the distributed form is elaborately delineated in the upcoming section. Initially, there are*n*data-point are assumed in the system where each i^{th}data-points has it's own secret key $S_i$and public keyP_i. The distributed ElGamal cryptosystem is comprised of the following algorithms.

3.1.1. Key generation

The first step in the cryptosystem is to generate a common public key (P_i) whichis utilized in thedistributed ElGamal cryptosystem and it has been depicted as follows,

$$PK=\prod_{i=1}^{n} S_i = g^{P_1+\ldots+P_n} \tag{3.1}$$

3.1.2. Encryption

The second stepin the cryptosystem is to encrypt a communicative plaintext message, ($M \epsilon G$), and aninteger R is chosen in a random manner from Z_q^* and after then the cipher text computation becomes: $CT_1 = g^R$ and $CT_2 = g^M \cdot PK^R$.The encrypted message (cipher text) is computed as

$$E(M) = (CT_1, CT_2) \tag{3.2}$$

3.1.3. Decryption

Here, a mutual decryption key is not ciphered. Each data-pointgenerates its ciphertext and disseminates partially decrypted estimates, and the final original/desired plaintext is disclosed by aggregating all partiallydecrypted estimates. For the ciphertext (CT_1, CT_2), decryption proceeds as follows:

- Every i^{th} data-points computes, $CT_1^{S_i}$;
- All the data-points disseminates committal estimated values $H(CT_1^{S_i})$;
- Now, each i^{th} data-points distributes $CT_1^{S_i}$and verifies if each$CT_1^{S_i}$copes with $H(CT_1^{S_i})$;
- Finally, each data-points computes,

$$\frac{CT_2}{\prod_{i=1}^{n} CT_1^{S_i}} = \frac{CT_2}{CT_1^{S_1+\cdots+S_n}} = g^M \tag{3.3}$$

- Finally,M will be disclosed by estimating the discrete logarithm.

3.1.4. Homomorphic Property

ElGamal encryption process has ahereditary homomorphic attribute[46], which admits exponentiation andmultiplicationto be executed on a set of required ciphertexts without any decryption, such as multiplication based homomorphic computation,

$$E(M_1)^{M_2} = (g^{R_1}, g^{M_1} \cdot PK^{R_1})^{M_2}$$
$$= (g^{R_1 \cdot M_2}, g^{M_1 \cdot M_2} \cdot PK^{R_1+M_2})$$
$$= E(M_1 + M_2) \quad (3.4)$$

and addition based homomorphic computation,

$$E(M_1) \times E(M_2) = (g^{R_1}, g^{M_1} \cdot PK^{R_1}) \times (g^{R_2}, g^{M_2} \cdot PK^{R_2})$$
$$= (g^{R_1+R_2}, g^{M_1+M_2} \cdot PK^{R_1+R_2})$$
$$= E(M_1 + M_2) \quad (3.5)$$

4. SYSTEM MODEL

In the proposed model, it is assumed that there are numerous *(dp)* organizations/data-points $\{D_1, D_2 \ldots\ldots, D_{dp}\}$. Since the decentralized network model is presumed, here each intra and inter data-points of any organization are allowed to collaborate, especially for encrypted communication. Each of them encrypts their data, and upon encryption transmits the ciphertext to the Central data-point *(Cdp)* where vital computation is performed. These computations are performed based on homomorphic operations.The *Cdp*determines the encrypted outcomes andtransmits it back to its parent organization without gaining knowledge on any privateselective information of the organizations.

The commencement of the crypto process starts from key generation, where each *dp* generates its key pairs (S_i, P_i) and transmit the P_i to the *Cdp*. Later then,*Cdp* combines the entirereceived $P_i$to acquire the master P_i which is distributed to all *dp*. This master P_i is utilized to encryptindividual private data. On receiving the encrypted ciphertext, the *Cdp* then executes homomorphic operationsto obtain thecombined encrypted outcomes which are apportionedamong the different *dp* in the network. The organizations then cooperateto decrypt the outcomes with the aid of *Cdp* utilizing their own$S_i$without disclosing any private data to the *Cdp*of other organizations. Basedon the decrypted results and its analysis make the organizations examine the impacts of cyberactivities if any and also lead a way to prevent secure data from external threats.

5. PERFORMANCE ANALYSIS

The observational analysis is sectioned into two primary segments.Firstly, the complexity of the proposed schema is discussed concerning communication and computation costs.

Secondly, based upon the computational complexities, few experiments are executed and exhibitthe bandwidth and actual time utilizedforprocessing the entire proposed schema. The complexity analysis includes the analysis of encryption/decryption and the message transmission costs for the single execution. Here, it is assumed that single encryptionin the ElGamal cryptosystem is always equivalent to $2m_E$ where$m_E$denotes modular exponentiation. Let, one homomorphic multiplication, homomorphic addition, and discrete logarithmfor decryption represented as h_{add}, h_{mul} and$\sqrt{T}m_E$respectively.Here,Tdenotes the size of the plaintext that needs to be encrypted or decrypted. Theunits of communication and computationcosts are presumed to be bits and seconds respectively. To test the performance is tested and evaluated using spam emails. Initially, the dataset of spam emails is randomly split into 20 different sets which are represented as 20different organizations. For evaluating the performance spam assassin datasetis utilized. Each organization bearing the subset of the dataset will execute the arbitrate computations and share the encrypted format outcomes with the *Cdp*. Upon receivingaggregated resultants from *Cdp*, each organization can generate and disclose, M by estimating the discrete.

5.1. Computation Complexity

At the commencement of experimental procedures, the *Cdp* gathers the entireP_i and createsa master P_i for all organizations. In this computation *Cdp* of each organizationperforms k multiplication over the public parameter as depicted in the equation. 3.1. Thus, the computation complexity of initialization procedures is presumed to be in k seconds.The organization transmits the encrypted data (ciphertexts) to its *Cdp.* Later then, each organizationexecutes two encryptions as depicted in the equation. 3.4with the complexity of $2m_E$ seconds.Now, the*Cdp* of each organization executes three different homomorphic additions, out of which two are executed for D organizations. Therefore, the complexitygets$2h_{add} \times D + h_{add}$ seconds. Then the *Cdp*determines theminimum outcomesbetween the n ciphertexts.Afterward, the outcome ciphertextsare disseminated to the organizations, where they handle the decryption technique to decrypt the resultslocally, which tends torender the complexityof $m_E + D \times m_E$. Each organization blots out their secretkeys S_k by advancing the ciphertext to the power of S_k, and performing D modular exponentiation.Eventually, the organization executesa discrete logarithm which brings $\sqrt{T} \times m_E$ seconds. Thus the decryption takes total complexity of $O(m_E + D \times m_{E+}$

$\sqrt{T} \times m_E$) seconds. Lastly, the total computation cost of each *Cdp* and the organization becomes $2h_{add} \times D + h_{add} + n$and $k + 2m_E + m_E + D \times m_E + \sqrt{T} \times m_E$seconds respectively.

5.2. Communication Complexity

For the evaluation of communication complexity, each generated ciphertexts that are to be exchanged among the various *Cdp's* of different organizations, and all these ciphertexts are assumed as *T* bits. At the initial phase, the *Cdp* gets the P_i from all organizations. Therefore it carries$D \times T$bits.As per the proposed scheme, each organization transmits two pairs of ciphertexts tothe *Cdp*. Now the communication costs become *4T* bits for each organization. The server receivesfrom *D* organization which results in $4T \times D$ bits to getthe ciphertexts. Later on, executing the homomorphic operations the*Cdp* disseminate a pair of ciphertext which is acquired byeach *D*of *2T* bits. Throughout the execution of the decryption process,the *Cdp* and each *D* exchange another set ofciphertexts which is depicted in the equation. 3.4. During this process, the bandwidthdemand becomes*2T* bits for each organization and $2T \times D$bits for the *Cdp*. Therefore, the total data/information essential for each *D* and *Cdp*is*7T* and $7D \times T$ bits respectively.

5.3. Efficiency

Table 1. Computational Complexity (in Time and Communication)

	Computation Complexity	Communication Complexity
Data-Points	$2h_{add} \times D + h_{add} + n$	7T
Organization	$k + 2m_E + m_E + D \times m_E + \sqrt{T} \times m_E$	7D × T
	Cost in Seconds	**Cost in MB**
Data-Points	20	0.0011
Organization	20	0.03

Table 1 depicts the performance outcomes of the proposed schemafor data-points and organization. For experimental analysis, 20 organizations and 20 different ciphertexts are considered, therefore, $D = 20$ and $T = 20$ respectively. Out of this presumed ciphertext, the *Cdp's* of each organization has to perform the comparison process to determine the minimum value without knowing the actual value. In the experimental setup,one homomorphic addition, and one modular exponentiationtakes about5.7 × 105 and 2 × 105 seconds respectively. On utilizing this setup, the entire schema process which comprises the mentioned server and each organizationtakesabout 20 seconds forfull completion. Figure 1demonstrates the scalability of

the proposed schemabyenhancing the count of organizations as per the requirement of applications. The result shows that there is a significant increase in the computation time as the count of the organization increases. However, the computation time of data-points seems not in the increasing mode, since the numberof ciphertexts for comparison purposes was limited to 20.

6. CONCLUSION

In this research article, a privacy-preserving schema has been proposed to enable secure communication in the decentralized network infra. Thus, on utilizing the homomorphic encryptions, proactive cyber defense is employed in an organization against harmful email. Although this is a simple approach to implement the specialized encryptions over a suitable datasetthe real challenges existed during decryption without exposing any private information while sharing them with other *Cdp's* of a different organization. Thus, the proposed schema addresses and overcomes these challenges through the deployment of homomorphic encryptions based ElGamal cryptosystem. This schema can be deployed to other types of numerical value based cyber threats dataset, since homomorphic encryptions highly support the features of numerical values like phishing data, but cannot be employed to fractional values. The proposed schema canbe of great usage for a proactive cyber defense system as it cansecure the dataset in a secured communication manner through strong encryption techniques.Asa future enhancement, collaborative, andproactive cyber defense systems using unsupervised machinelearning algorithms are consideredina privacy-preserving manner. In-depth privacyexaminationand investigation on experimental outcomes of proposed schemaexhibit the practicalityas well as security.

REFERENCE

1. J.-M. Seigneur, Collaborative Computer Security and Trust Management.IGI Global, 2009.
2. Vakilinia, D. K. Tosh, and S. Sengupta, "3-way game model forprivacy-preserving cybersecurity information exchange framework," inMilitary Communications Conference (MILCOM), MILCOM 2017-2017IEEE. IEEE, 2017, pp. 829–834.
3. Vakilinia and S. Sengupta, "A coalitional game theory approachfor cybersecurity information sharing," in Military CommunicationsConference, MILCOM 2017-2017 IEEE. IEEE, 2017, pp. 237–242.

4. Vakilinia, D. K. Tosh, and S. Sengupta, "Privacy-preserving cybersecurityinformation exchange mechanism," in Performance Evaluationof Computer and Telecommunication Systems (SPECTS), 2017 InternationalSymposium on IEEE, 2017.

5. Vakilinia and S. Sengupta, "A coalitional cyber-insurance frameworkfor a common platform," IEEE Transactions on Information Forensicsand Security, 2018.

6. Vakilinia, S. Cheung, and S. Sengupta, "Sharing susceptible passwordsas cyber threat intelligence feed," in Military CommunicationsConference (MILCOM), MILCOM 2018-2018 IEEE, 2018.

7. R. Bye, S. A. Camtepe, and S. Albayrak, "Collaborative intrusion detectionframework: Characteristics, adversarial opportunities, and countermeasures."in CollSec, 2010.

8. C. V. Zhou, C. Leckie, and S. Karunasekera, "A survey of coordinatedattacks and collaborative intrusion detection," Computers & Security,vol. 29, no. 1, pp. 124–140, 2010.

9. V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey,"ACM computing surveys (CSUR), vol. 41, no. 3, p. 15, 2009.

10. H. T. Elshoush and I. M. Osman, "Alert correlation in collaborativeintelligent intrusion detection systemsa survey," Applied Soft Computing,vol. 11, no. 7, pp. 4349–4365, 2011.

11. G. Caruana and M. Li, "A survey of emerging approaches to spamfiltering," ACM Computing Surveys (CSUR), vol. 44, no. 2, p. 9, 2012.

12. Wang, F., and Vergara-Niedermayr, C. 2009. CollaborativelySharing Scientific Data. Collaborative Computing:Networking, Applications, and Worksharing. E. Bertino andJ.D. Joshi, eds. Springer Berlin Heidelberg. pp.805–823.

13. Ives, Z.G. et al. 2008. The ORCHESTRA Collaborative DataSharing System. ACM Special Interest Group onManagement of Data (SIGMOD) Record. 37, 3 (Sep. 2008),26–32.

14. Simpson, A. et al. 2010. On the Secure Sharing andAggregation of Data to Support Systems Biology Research.Data Integration in the Life Sciences. P. Lambrix and G.Kemp, eds. Springer Berlin Heidelberg. pp. 58–73.

15. Li, F. et al. 2013. Enforcing Secure and Privacy-PreservingInformation Brokering in Distributed Information Sharing.Information Forensics and Security, IEEE Transactions on.8, 6 (Jun. 2013), pp. 888–900.

16. Rodríguez-Gianolli, P. et al. 2005. Data Sharing in theHyperion Peer Database System. Proceedings of the 31st International Conference on Very Large Data Bases (2005), 1291–1294.

17. Ng, W.S. et al. 2003. PeerDB: a P2P-based system for distributed data sharing. Data Engineering, 2003. Proceedings. 19th International Conference on (Mar. 2003), pp. 633–644.

18. Clarke, I. et al. 2001. Freenet: A distributed anonymous information storage and retrieval system. Designing Privacy Enhancing Technologies (2001), pp. 46–66.

19. Elmeleegy, H. et al. 2010. Preserving privacy and fairness in peer-to-peer data integration. Proceedings of the ACM Special Interest Group on Management of Data (SIGMOD) International Conference on Management of data (2010), pp. 759–770.

20. Masud, M.M. et al. 2005. Don't Mind Your Vocabulary: Data Sharing Across Heterogeneous Peers. On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE. R. Meersman and Z. Tari, eds. Springer Berlin Heidelberg. pp. 292–309.

21. Martinelli, F. et al. 2012. A Formal Support for Collaborative Data Sharing. Multidisciplinary Research and Practice for Information Systems. G. Quirchmayr et al., eds. Springer Berlin Heidelberg. pp. 547–561.

22. Higgins, M., 2006. Managing Distributed Collaboration in a Peer-to-Peer Network. On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE. R. Meersman and Z. Tari, eds. Springer Berlin Heidelberg. pp. 569–586.

23. Gatterbauer, W., 2009. Believe It or Not: Adding Belief Annotations to Databases. Proceedings of the Very Large Database (VLDB) Endowment. 2, 1 (Aug. 2009), pp. 1–12.

24. Gatterbauer, W., and Suciu, D. 2010. Data Conflict Resolution Using Trust Mappings. Proceedings of the ACM Special Interest Group on Management of Data (SIGMOD) International Conference on Management of data (New York, NY, USA, 2010), pp. 219–230.

25. Cheng, R. et al. 2005. U-DBMS: A Database System for Managing Constantly-evolving Data. Proceedings of the 31st International Conference on Very Large Data Bases (2005), pp. 1271–1274.

26. Iovino, G. et al. 2013. Federated Threat Data Sharing with the Collective Intelligence Framework (CIF). (Honululu, US, Jan. 2013).

27. Grobauer, B. et al. 2014. The MANTIS Framework: Cyber Threat Intelligence Management for CERTs. (Boston, US, Jun. 2014).

28. Socha, K. 2013. Effective Management and Sharing of Indicators of Compromise. (Warsaw, Poland, Oct. 2013).

29. Avalanche: 2014. http://avalanche.fsisac.com/. Accessed: 2014-07-25.

30. Gilman, R. 2013. Better Tools Through Intelligence, Better Intelligence Through Tools. MITRE Cyber Threat Analysis Cell.

31. GoodwinC,Nicholas JP (2015). AFrameworkforCybersecurity Information Sharing and Risk Reduction (Microsoft, Redmond, WA).

32. F. Brandt, "Efficient cryptographic protocol design based on distributed Elgamal encryption," in International Conference on Information Security and Cryptology. Springer, 2005, pp. 32–47.

33. Boyer, R., and Moore, J. A fast string searching algorithm. Communications of the ACM 20, 10 (1977), pp. 762–772.

34. Zhao, X., and Prakash, A. "WSF: An HTTP level Firewall for Hardening Web Servers. In Parallel and Distributed Computing and Systems" Proceedings of the 17th IASTED International Conference (2005).

35. Landwehr, C., Bull, A., Mcdermott, J., And Choi, W. "Taxonomy of computer program security flaws". ACM Computing Surveys (CSUR) 26, 3 (1994), pp. 211–254.

36. Xiao-Feng Wang, Jing-Li Zhou, S. S. Y., And Cai, L. Z. Data Mining Methods for Anomaly Detection of HTTP Request Exploitations. In Proceedings of Springer Verlag Berlin Heidelberg 2005, Springer.

37. Raskin V., C.F. Hempelmann, K.E. Triezenberg, Nirenburg, "Ontology in Information Security: A Useful Theoretical Foundation and Methodological Tool," Proceedings of the 2001 Workshop on New Security Paradigms (NSPW-2001), pp. 53-59, 2001.

38. Ning, P., Jajodia, S., and Wang, X. "Abstraction based intrusion detection in distributed environments", ACM Transactions on Information and System Security (TISSEC), 4 (2001), pp. 407– 452.

39. Mchugh, J.: "Intrusion and intrusion detection". International Journalof Information Security 1, 1 (2001), pp. 14–35.

40. Lough, D. "A taxonomy of computer attacks with applications towireless networks". Ph.D. thesis,2001.

41. Denker, G., Kagal, L., Finin, T., Paolucci, M., and Sycara, K. "Securityfor daml web services: Annotation and matchmaking". The SemanticWeb ISWC 2003 (2003), pp. 335–350.

42. Daml.Org, Daml,Oil. WWW page, December 2000.

43. Fenz, S., and Weippl, E. Information Security Fortification byOntological Mapping of the ISO/IEC 27001 Standard, 2008.

44. Fong, E., and Okun, V. “Web Application Scanners: Definitions andFunctions”. In System Sciences, 2007. HICSS 2007. 40th AnnualHawaii International Conference on (2007), IEEE, pp. 280b– 280b.

45. Bartel M., Boyer, J., Fox, B., Lamacchia, B., and Simon, E.: “XMLsignaturesyntax and processing”. W3C recommendation, 2002.

46. X. Yi, R. Paulet, and E. Bertino, Homomorphic encryption and applications.Springer, 2014, vol. 3.

47. O. Serrano and L. Dandurand and S. Brown, “On the Design of a Cyber Security Data Sharing System”, WISCS '14, 2014.